The Ohio State Technology Law Journal

# RESTRAINING THE SURVEILLANCE SOCIETY: COMPARING PRIVACY POLICIES FOR AUTOMATED LICENSE PLATE READERS IN THE UNITED STATES AND THE UNITED KINGDOM

KEARSTON WESNER* AND KATIE BLEVINS*

* Kearston L. Wesner is an Associate Professor of Media Studies at Quinnipiac University. Her research uses the lens of new technologies to explore the intersection of privacy and the First Amendment.

* Katie Blevins is an Assistant Professor in the School of Journalism and Mass Media, and the Co-Director of the Women's, Gender & Sexuality Studies program, at the University of Idaho. Her legal research focuses on issues of government transparency and access to information.

CONTENTS

## INTRODUCTION

In May 2020, the Ninth Circuit addressed an increasingly pressing question: when law enforcement uses automated-license plate reader (ALPR)[1] technology without a warrant, does this constitute a search in violation of the Fourth Amendment right to privacy?[2] The case, *United States v. Yang*, centered on a man caught on a surveillance camera over the course of several days exiting two vehicles and removing mail from a locked collection box in Nevada.[3] He appeared to be engaged in the practice called "fishing," which involves stealing mail by inserting an object reinforced with adhesive or modified with a grabbing "claw" into a mailbox.[4] The surveillance footage showed both vehicles' license plate numbers.[5] Law enforcement checked this information against a license plate-location database called LEARN.[6]

The information in the LEARN database was collected by ALPRs. ALPRs, which can either be mobile (affixed to vehicles, as in the *United States v. Yang* case) or stationary (on fixed structures such as utility poles), automatically capture license plates that come into the camera's frame, recording a vehicle's plate number, time of collection, and location of the vehicle.[7] The private LEARN database, owned by Vigilant Solutions, currently contains more than 6.5 billion license plate scans gathered by digital cameras on "tow truck, repossession company and law enforcement vehicles."[8] Access to the database is limited to an elite group of people: law enforcement officers who pay a subscription

[1] This technology is also referred to in the literature – specifically U.K. scholarship, as is pertinent to this paper – as automatic number-plate recognition (ANPR) technology.
[2] United States v. Yang, 958 F.3d 851, 853 (9th Cir. 2020).
[3] *Id.* at 854.
[4] *Id.*
[5] *Id.*
[6] *Id.* at 855.
[7] ALPR data typically includes the following: black-and-white and color plate images, plate numbers in electronically readable, location and GPS coordinates, the time and date of image capture, and camera identification information. DAVID J. ROBERTS & MEGHANN CASANOVA, AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS: POLICY AND OPERATIONAL GUIDANCE FOR LAW ENFORCEMENT 12 (2012).
[8] United States v. Yang, 958 F.3d 851, 855 (9th Cir. 2020).

fee.[9] The Postal Inspection Service, which was investigating the mail theft, fell in this group.[10]

By matching the surveillance camera footage of the license plate numbers to information in the LEARN database, the Postal Inspection Service was able to identify the mail-theft suspect as Jay Yang.[11] Ultimately, law enforcement officers obtained a search warrant for Yang's home and discovered fishing devices, many pieces of stolen mail, and a firearm.[12] Yang sought to suppress this evidence, asserting that the search warrant hinged on illegally-obtained evidence: the ALPR data.[13] The court declined to allow suppression, holding that Yang had no reasonable expectation of privacy that was compromised by the use of ALPR technology.[14] License plate information, after all, is publicly viewable, and there is historically no expectation of privacy in public.[15]

The issues presented in *United States v. Yang* are especially pertinent given the current landscape. In the past few years, ALPRs have been increasingly deployed in the U.S. by both law enforcement and private industry. This increased dependence on surveillance technology reflects the trend in many other countries, including the United Kingdom.

As *United States v. Yang* illustrates, law enforcement has found tremendous value in the information yielded by ALPRs.[16] This simple

---

[9] *Id.*
[10] *Id.*
[11] *Id.* at 854.
[12] *Id.* at 857.
[13] *Id.*
[14] *Id.* The court rejected Yang's arguments that he had a reasonable expectation of privacy in his movements that was violated by the use of ALPR technology. In part, the court was motivated by the fact that the vehicle at issue was a rental, and Yang's privacy expectations were informed in large part by the rental agreement. *Id.*
[15] *Id.*
[16] The technology is not limited to law-enforcement use, however. Private businesses such as repossession companies also have adopted the technology to streamline business costs and simplify the process of locating vehicles. Companies such as Michigan-based Vigilant Technologies use ALPRs to capture and sell license-plate information to police agencies and private companies. Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC (Apr. 22, 2016),

and relatively inexpensive technology is hardly limited to revealing petty mail theft; it can be used for many purposes including detecting stolen vehicles, locating drivers with active warrants or expired licenses, and ascertaining whether a specific vehicle was involved in a crime.[17] Additionally, the private sector has also found commercial value in the collection of ALPR data. For example, insurance companies have used ALPR technology to track insurance fraud,[18] and repossession firms have used it to locate vehicles when their owners failed to make payments.[19] Furthermore, homeowners associations and gated communities have also embraced ALPR technology to monitor vehicles entering and leaving their neighborhoods.[20]

ALPR technology undeniably can simplify law enforcement procedures, aid private companies in conducting their business, and help secure community safety. But its use poses significant privacy concerns that arguably outweigh the benefits. Some of these concerns are particular to the law enforcement context. For example, some law enforcement officers have abused their "surveillance discretion"[21] by

---

https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/ [https://perma.cc/2DW7-PQEA].

[17] ROBERTS & CASANOVA, *supra* note 7, at 1. In a 2012 report on ALPR use to the U.S. Department of Justice, the authors identified some of the various uses of ALPR data for law enforcement: "[a]s noted, law enforcement practitioners are often searching for vehicles that have been reported stolen, are suspected of being involved in criminal or terrorist activities, are owned by persons who are wanted by authorities, have failed to pay parking violations or maintain current vehicle license registration or insurance, or any of a number of other legitimate reasons." *Id*.

[18] Sam Boyer, *License Plate Recognition Is Helping Insurers Catch Fraud*, INS. BUS. AM. (Jun. 5, 2017), https://www.insurancebusinessmag.com/us/news/commercial-auto/license-plate-recognition-is-helping-insurers-catch-fraud-69487.aspx [https://perma.cc/X9WG-FAC5].

[19] Joseph Cox, *This Company Built a Private Surveillance Network. We Tracked Someone with It*, MOTHERBOARD (Sept. 17, 2019, 10:45 AM), https://www.vice.com/en/article/ne879z/i-tracked-someone-with-license-plate-readers-drn [https://perma.cc/6Y2V-FVEN].

[20] Elise Schmelzer, *Denver-Area Neighborhoods Are Installing License Plate Readers to Record Every Vehicle that Passes by*, DENVER POST (July 15, 2019, 7:10PM), https://www.denverpost.com/2019/07/09/license-plate-reader-hoa-colorado-flock-safety [https://perma.cc/44GL-4FEF].

[21] Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 15 (2016).

targeting the use of ALPR technology to low-income areas[22] or in communities of color.[23] These concerns are amplified by reports of "misreads" by ALPR technology, which could have tremendous consequences for those erroneously targeted.[24] In both the law enforcement and private contexts, there are also serious concerns about the breadth of data collection, leading to accusations of overreach.[25]

ALPR databases typically contain information about *all* vehicles recorded, even those irrelevant to the central investigation or dispute.[26] Furthermore, investigations have revealed serious data breaches due to inadequate security. In 2015, the entire Boston, Massachusetts ALPR network was rendered vulnerable after a security lapse, making all users' records since 2012 freely accessible.[27] These egregious privacy concerns were echoed in a 2015 Electronic Frontier Foundation investigation and a 2019 TechCrunch study, both of which discovered

---

[22] Dave Maass & Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, ELEC. FRONTIER FOUND. (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data [https://perma.cc/68AC-VP2A].

[23] *See, e.g.,* Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, HUFFINGTON POST (Apr. 25, 2012), https://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html [https://perma.cc/967J-GY33]; Russell Brandom, *Exclusive: ICE Is About to Start Tracking License Plates Across the U.S.*, VERGE (Jan. 26, 2018, 8:04 AM), https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions [https://perma.cc/75NY-VK38].

[24] *See, e.g.,* Tim Cushing, *Deputies Sued After False ALPR Hit Leads to Guns-Out Traffic Stop of California Privacy Activist*, TECHDIRT (Feb. 20, 2019, 10:43 AM), https://www.techdirt.com/articles/20190217/08240241618/deputies-sued-after-false-alpr-hit-leads-to-guns-out-traffic-stop-california-privacy-activist.shtml [https://perma.cc/3JKP-MEKT].

[25] *See* Barry Friedman & Elizabeth G. Janszky, *Policing's Information Problem,* 99 TEX. L. REV. 1, 19 (2020).

[26] LEARN captures data on all recorded vehicles, even those that are not (1) linked to the commission of a crime or (2) connected to a person suspected of criminal activity. *See* United States v. Yang, 958 F.3d 851, 855 (9th Cir. 2020).

[27] Kenneth Lipp, *License to Connive: Boston Still Tracks Vehicles, Lies About It, and Leaves Sensitive Resident Data Exposed Online*, DIGBOSTON (Sept. 8, 2015), https://digboston.com/license-to-connive-boston-still-tracks-vehicles-lies-about-it-and-leaves-sensitive-resident-data-exposed-online [https://perma.cc/LV48-QKVE].

that the information obtained by ALPR devices was secured inadequately and readily accessible to the public.[28]

There are two troubling developments with regard to widespread ALPR adoption. First, the use of ALPRs to conduct mass surveillance has received little scholarly legal analysis[29] and "is not typically considered activity reached by the Fourth Amendment at all."[30] Second, despite the serious privacy concerns raised by the deployment of ALPR technology, government response has been inadequate and/or inconsistent.[31] To illustrate how wildly divergent the approaches are, one need only assess the policies adopted by the U.K. and the U.S.

In the U.S., as in the U.K., legislators have wrestled with the privacy implications of increased dependence on surveillance technology by both law enforcement and private industry. But the countries' responses have varied. The U.K. – a country often called "one of the most surveilled nations in the world"[32] – has developed broad, detailed legislation (bolstered by European Union regulations) to protect individual privacy. In contrast, the U.S. has adopted a patchwork approach to regulation, resulting in myriad disparate laws that fail to address privacy concerns adequately.[33]

---

[28] Cooper Quintin & Dave Maass, *License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech*, ELEC. FRONTIER FOUND. (Oct. 28, 2015), https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive [https://perma.cc/U29F-9DVB]; Zack Whittaker, *Police License Plate Readers Are Still Exposed on the Internet*, TECHCRUNCH (Jan. 22, 2019, 6:26 PM), https://techcrunch.com/2019/01/22/police-alpr-license-plate-readers-accessible-internet [https://perma.cc/R3DE-THYQ].

[29] Joh, *supra* note 21, at 18.

[30] *Id.* at 19 (construing United States v. Wallace, 811 F. Supp. 2d 1265, 1272 (S.D. W. Va. 2011)).

[31] Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Reader: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CENTER (Sept. 10, 2020), https://brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations [https://perma.cc/5Y6R-WZ42].

[32] James Temperton, *One Nation Under CCTV: The Future of Automated Surveillance*, WIRED (Aug. 17, 2015, 7:38 PM), http://www.wired.co.uk/article/one-nation-under-cctv [https://perma.cc/7S2H-XNVT].

[33] Lydia Bayley, *The Patchwork Paradox: Data Privacy Regulation and the Complications of Compliance*, LOYOLA U. CHI.: INSIDE COMPLIANCE (Sept. 1, 2020), http://blogs.luc.edu/compliance/?p=3142 [https://perma.cc/7E8Q-KVAS].

These disparate policies form the foundation of this study. The study has two overarching aims: (1) to compare and contrast the ALPR data collection, retention and use policies in the U.S. and the U.K., and (2) to articulate clear guidelines that ensure accountability regarding the use and retention of citizens' data. To accomplish these goals, this study uses traditional legal research methodology. First, this study explores the foundation of privacy regulation in the U.S. and the U.K. Second, the study examines the relationship between the deployment of ALPR technology and privacy considerations. Third, the study analyzes the existing status of U.K. and U.S. governance with respect to ALPR technology and privacy. Finally, this study provides policy recommendations for entities using ALPR technology.

Throughout, the study primarily focuses on the law enforcement versus the private industry context in the discussion of these issues; the majority of the legal and regulatory issues surrounding ALPRs have so far arisen in the law enforcement context. However, many of the issues addressed in the study are directly applicable to private industry as well. This study ultimately both guides privacy advocates and scholars in the U.K. and the U.S. and provides comparative understanding to other scholars working in countries with similar common law approaches to this technology.

Surprisingly scant research has been directed at this area. The bulk of the research has centered on the U.S. Constitution, particularly Fourth Amendment issues of unreasonable searches and seizures, as illustrated by the *United States v. Yang* case explored above.[34] The facts of *United States v. Yang* notwithstanding, the use of ALPRs themselves – gathering data to determine *whether* to conduct a later search – does not typically implicate Fourth Amendment concerns about search and seizure. Instead, the privacy concerns focus mainly on the bulk collection of ALPR data by law enforcement, inadequate or unclear storage practices, and broad use of this data to establish patterns of

[34] United States v. Yang, 958 F.3d 851, 858-59 (9th Cir. 2020).

activity or reveal misconduct unassociated with the original data collection.

While most of the scholarship and case law focuses on law enforcement use of ALPR technology, private companies' collection, storage, and use practices also trigger privacy concerns. Additionally, the widespread and relatively unrestrained use of this technology raises generalized privacy concerns outside of any one country's legal framework. This study hopes to provide an outline of potential problems and a framework to create reasoned guidelines regarding the use of ALPRs.

## I. THE FOUNDATION OF PRIVACY LAW IN THE U.S. AND THE U.K.

This study explores the deployment of ALPRs and the concomitant technological and privacy concerns that deployment raises. To understand the varied legislative approaches adopted by the U.S. and U.K. regarding ALPRs, it is instructive to focus first on these countries' philosophical approaches to privacy. In both countries, the societal expectations of personal privacy inform the legislative response to ALPR technology, which forms the basis of this study.

Contemporary definitions of privacy draw on tightly embedded links between "self-determination, autonomy, dignity, surveillance, power, and technology."[35] This conceptualization of privacy drives legislative approaches in both the U.S. and the U.K.[36] The ability to defend personal information – and shield those embedded links – becomes more pressing in the current global information society, where "almost all attributes of an individual can be known… [and] *all interactions*

---

[35] GUS HOSEIN, *Privacy as Freedom*, *in* HUMAN RIGHTS IN THE GLOBAL INFORMATION SOCIETY 124 (2006).

[36] *See, e.g.*, David Banisar et al., *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, GLOBAL INT. LIBERTY CAMPAIGN gilc.org/privacy/survey/intro.html [https://perma.cc/FZ5U-UVPL]; Yvonne McDermott, Commentary, *Conceptualising the Right to Data Protection in an Era of Big Data*, BIG DATA & SOC'Y (Jan. 1, 2017), https://journals.sagepub.com/doi/full/10.1177/2053951716686994 [https://perma.cc/C5HW-GWTK].

*mapped*."[37] The issue of ALPRs becomes more complicated on a global scale because the technology straddles multiple aspects of privacy law and multiple jurisdictions. Courts and lawmakers have generally found that certain factors are echoed in various international laws: use of the technical device,[38] place,[39] intensity,[40] duration,[41] degree of suspicion,[42]

[37] HOSEIN, *supra* note 35, at 124 (emphasis added).
[38] Bert-Jaap Koops et al., *Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance'*, 9 U.C. IRVINE L. REV. 635, 677 (2019). Most courts have acknowledged that technology-facilitated surveillance will have a greater impact on privacy than human perception-based surveillance. While the use of technical surveillance is not necessarily automatically problematic legally, it does contribute to a scope shift under privacy considerations. *Id.*
[39] *Id.* at 679. Generally, surveillance in public places is less of a burden on privacy than surveillance in private places. ALPR technology often receives less scrutiny because it is used on public roadways. *Id*.
[40] *Id.* at 680. Intensity consists of the depth of surveillance, the continuity of the surveillance, and the frequency of the surveillance. *Id.* ALPR technology is used in different ways that calls these aspects of intensity more and less into account. For example, a fixed ALPR camera on a light pole does not provide continuity or surveillance because it does not follow a single license plate, but it could provide frequency of surveillance if the camera is located on a route that a local driver takes several times a day. Similarly, while ALPR databases on their own only constitute license registrations, they are often linked to other related law enforcement, public, and even private sector databases, providing a depth of surveillance that falls outside of a functional understanding of license place registration.
[41] *Id.* The longer someone is tracked, the more intrusive it is. *Id.* With ALPR technology, unless a suspect is actively tracked using their license plate, this technology generally is not as intrusive as a GPS tracker affixed to their car. That being said, data retention can establish patterns over time, essentially mapping citizens' general movements. This is why most privacy advocates request that ALPR data be wiped routinely, to minimize concerns about the duration of tracking.
[42] *Id.* at 681-82. Some courts internationally hold that people lose a measure of their expectation to privacy based on the likelihood of their involvement in criminal activity. *Id.* With regards to ALPRs, "hot lists" and "hot spots" are merely identifying individuals and places where crime is more likely to occur and does not heavily infringe on privacy concerns since people committing criminal activities have a reduced expectation to privacy. This is a contested approach to privacy law from a profiling, systemic discrimination perspective.

object of tracking,[43] covertness,[44] and active generation of data.[45] Taken as a whole, these factors speak to continued legal uncertainty about the tension between existing privacy expectations and the role of new information-gathering technology.

As explained below, the U.S. has historically conceptualized privacy as an interest of bodily autonomy, cast as the "right to be let alone," which has been narrowed over time to a right to be alone in your personal space – the home. The U.K. historically has grounded its privacy analysis in the individual right to secure one's home from intrusion. The rights in both countries have expanded slowly to encompass informational privacy. The historical conceptualization of privacy in both countries continues to drive the discussion of privacy and, by extension, privacy legislation, and do not account for the current information age.

### *A. Privacy Law in the U.S.*

The right to privacy was first formally articulated in the U.S. in 1890 by Samuel Warren and Louis Brandeis in response to the dangers posed by Kodak's "snap camera."[46] Driven by the concern that new technologies threaten individual privacy, Warren and Brandeis argued that the law should provide adequate protections.[47] In their analysis, they conceptualized privacy as the right to be left alone.[48] This conceptualization of privacy as a negative right has influenced the development of privacy legislation.

---

[43] *Id.* at 682. Generally, tracking an object is seen as less intrusive to privacy than tracking a person. *Id*. ALPR technology tracks specific license plates but cannot discern who is driving the car at any specific point. This information is cross-referenced with other databases though, and police are often aware of driver descriptions, names, etc. if they pursue a traffic stop.

[44] *Id.* at 683. International law is more split on whether covert surveillance represents less or more privacy concerns. For example, under Dutch law overt and covert surveillance is equally intrusive. *Id.* Under U.K. law, covert surveillance is seen as more problematic to surveillance than overt. *Id.* In Italy, overt tracking is seen as more intrusive than covert tracking. *Id*.

[45] *Id.* at 683-84. This factor is central to U.S. privacy law and related to active versus passive data collection. When law enforcement passively acquire data, it is seen as less intrusive than when they actively cause data to be generated. *Id.* This distinction is why there is sometimes a preference for fixed/stationary ALPR cameras vs. mobile ALPR cameras mounted to police squad cars.

[46] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[47] *Id.* at 195-96.

[48] *Id.* at 193-95.

Warren and Brandeis's article ultimately transformed the legal landscape and has become one of the most cited law review articles in history.[49] But the initial response to the article was sluggish, at best.[50] At the time, the law was not developed to provide relief for mental anguish, and privacy invasions did not "contain[] an anchor in property," which would be necessary for injunctive relief.[51] The foundations of the legal system had to shift before it could accommodate the privacy torts proposed by Warren and Brandeis.[52]

By 1960, this shift had occurred.[53] Legal scholar and law professor William Prosser categorized four torts to protect privacy: intrusion, public disclosure of private facts, false light, and appropriation.[54] Though hardly the first scholar to tackle this task, Prosser has been credited with transforming the legal landscape.[55] The privacy taxonomy outlined in his article, *Privacy*, became part of the Restatement (Second) of Torts.[56] The conceptualizations inked in Prosser's article continue to guide legal analysis more than 60 years after its publication.[57]

More than a century has passed since Warren and Brandeis's influential article, during which privacy has been re-envisioned periodically. It has been reimagined as a property right[58] or as encompassing the right to control private information.[59] And as predicted by Warren and

---

[49] *See* Fred R. Shapiro, *The Most Cited Law Review Articles Revisited,* 71 CHI.-KENT L. REV. 751 (1996).
[50] *See* William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 388-89 (1960).
[51] Jared A. Wilkerson, *Battle for the Disclosure Tort*, 49 CAL. W. L. REV. 231, 237 (2013) (asserting that to pave the way for robust privacy protections, it was necessary to first "rectify inadequacies in the common law").
[52] *See* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1 (1979).
[53] *See* Prosser, *supra* note 50.
[54] *Id.*
[55] Vernon V. Palmer, *Three Milestones in the History of Privacy in the United States*, 26 TUL. EUR. & CIV. L.F. 70 (2011) (describing the milestones of Prosser in American tort law).
[56] *Id.* at 91.
[57] *See generally id.* at 91-92.
[58] *See* Prosser, *supra* note 53, at 401-02 (1960) (specifically, the tort for appropriation conceptualizes a person's name or likeness as property).
[59] *See* Riley v. California, 573 U.S. 373 (2014), (in which the Supreme Court unanimously held that warrantless searches and seizure of cellphones violated information privacy. The

Brandeis, technological developments have continued to spur both societal and legal transformations.[60]

The U.S. Supreme Court has struggled with how to protect privacy in the face of new technologies. In the U.S., the Constitution assumes precedence. U.S. law must contend with the tension between the protection of free expression, secured by the First Amendment, and the right of privacy, envisioned as a penumbral right to the First Amendment.[61] The interplay of these rights is interpreted via the Supreme Court and federal courts. How to handle these technologies is complicated in a landscape that defines privacy narrowly or grounds it in property rights developed to target and secure *physical* property. Thus, the court has struggled to articulate whether/how to protect privacy in cases involving the bulk collection of computerized data[62] or the use of devices such as GPS trackers[63] or thermal-imaging devices.[64]

### *B. Privacy Law in the U.K.*

In the U.K., privacy has historically been articulated in terms of securing a physical space in which one can remain free from intrusion.[65] This space is often conceptualized or defined as "the home."[66] This

ability to control personal information as an encompassing privacy right is not yet settled. As information technologies have advanced, scholars continue to debate the amount of control individuals should expect); *see* Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUT. & HIGH TECH. L.J. 63 (2011); Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2003); Daniel E. Newman, *European Union and United States Personal Information Privacy and Human Rights Philosophy – Is There a Match?*, 22 TEMP. INT'L & COMP. L.J. 307 (2008).

[60] *A History of How Technology Has Transformed the Legal Field*, ZAPPROVED (Sept. 9, 2021), https://zapproved.com/blog/a-history-of-how-technology-has-transformed-the-legal-field/ [https://perma.cc/38EF-TL4G].

[61] Griswold v. Connecticut, 381 U.S. 479, 483 (1965) (the Court discussed this penumbra extending from the existing Bill of Rights); R.H. Clark, *Constitutional Sources of the Penumbral Right to Privacy*, 19 VILLANOVA L. REV. 833 (1974).

[62] *See* Whalen v. Roe, 429 U.S. 589 (1977).

[63] *See* United States v. Jones, 565 U.S. 400 (2012).

[64] *See* Kyllo v. United States, 533 U.S. 27 (2001).

[65] *See* HOSEIN, *supra* note 35.

[66] Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 CONN. J. INT'L L. 257, 268 (2013) (for example, in the United States,

approach can be found, for example, in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of 1950, which created the European Court of Human Rights and established a binding treaty on European definitions of human rights.[67] Article 8 addresses privacy as such: "[e]veryone has the right to respect for his private and family life, *his home* and his correspondence."[68] In this example, the emphasis on privacy as a human right is on ensuring the privacy of *home life*. There is no consideration of privacy in public; there is certainly no language addressing how mapping a person's movement in public places could impact personal privacy.[69]

Still, the legal right of privacy was not articulated in the U.K. Constitution until 1998, when it incorporated the European Convention of Human Rights into British law.[70] But one key difference to note between the U.S. and the U.K. is the principle of parliamentary supremacy.[71] Whereas the U.S. Constitution (as interpreted by the Supreme Court and federal courts) is the ultimate legal authority in the U.S., this is not the case in the U.K. The U.K. Constitution combines common law, statutory law, and custom.[72] In essence, no single document in the U.K. has total precedence, as it does in the U.S.[73]

Unlike the U.S., the U.K. has embraced an approach to privacy that imposes a positive obligation, primarily on the government and private companies, to secure individual data.[74] Privacy is conceptualized as the

---

individuals do not have an unequivocal fundamental right to individual privacy; instead, they have "highly conditional 'zones of privacy'," such as the expectation of privacy in the home).

[67] European Convention on Human Rights, Council Eur., Nov. 4, 1950.

[68] *Id.* (emphasis added)(a second part to Article 8 clarified that: "[t]here shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

[69] *See* HOSEIN, *supra* note 35.

[70] *See* HOSEIN, *supra* note 35*;* Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1153 (2006) (while specifically statutes protected aspects of privacy under British law, the 1998 incorporation offered blanket protection).

[71] Donahue, *supra* note 70, at 1152.

[72] *Id.*

[73] *Id.* at 1153.

[74] *Id.* at 1154.

"ability to control information and to choose whether and in what manner to communicate personal details."[75] Critical to this approach is the dominion over personal data and the right to secure that data against institutional abuse.[76] The philosophy is embodied in the EU's 2016 General Data Protection Regulation ("GDPR") law.[77] The GDPR aims to secure personal data (defined as "any piece of information that relates to an identifiable person" [78]) by focusing on this combination of positive obligation and fair information practices.[79]

This approach, however, is not bulletproof. The 1998 European Convention of Human Rights provides a loophole that broadly allows public authorities to intrude on individual privacy when needed for "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[80]

As such, the U.K. exists in a juxtaposition. The public culture is generally in favor of a positive approach to privacy law, and the GDPR protects personal data from corporations.[81] At the same time, the U.K. (and Great Britain specifically), is one of the most publicly surveilled places in the world.[82] In the early 2000s, the U.K. developed one of the

---

[75] *Id.* at 1154.
[76] HOSEIN, *supra* note 35, at 133 (this approach, also adopted in other countries' data protection laws, shields individuals from "abuse from both public agencies and privacy companies.").
[77] Commission Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119).
[78] Richie Koch, *What is Considered Personal Data Under the EU GDPR?*, GDPR.EU, https://gdpr.eu/eu-gdpr-personal-data/ [https://perma.cc/4KFP-X62N].
[79] *Id.* (while the databases continue to be magnified today, corollary fair information practices have mostly languished, with many countries failing to incorporate options for informed consent of individuals, fair and lawful collection of data, limited use and retention of data, secure and accurate storage, and lack of transfer to third parties); HOSEIN, *supra* note 35, at 133-34 (data protection laws started to develop internationally in the 1960s, mostly in response to increasingly elaborate secret databases which held large amounts of information about private citizens).
[80] Donohue, *supra* note 70, at 1155.
[81] *Id.* at 1184.
[82] *Id.*

most advanced closed-circuit television (CCTV) networks in the world.[83] As of 2004, there were over 4 million CCTVs operating in Britain; the average person traveling through London is captured on film 300 times in a single day.[84] As technology has advanced, the cameras have been upgraded to incorporate facial recognition software to scan law enforcement databases.[85] Against these different cultural and legal backdrops, comprehensive policies for emerging technology like ALPRs are difficult to create.

## II. THE PRIVACY IMPLICATIONS OF ALPR DATA COLLECTION AND USE PRACTICES

ALPR technology has been deployed to conduct wholesale community surveillance, tracking the movements of all individuals for all purposes.[86] Ordinarily, the maxim applies that there is no expectation of privacy in public.[87] But should this maxim be updated to exclude or limit mass surveillance, particularly when the aggregated data reveals extraordinarily personal information about an individual?

Both public and private actors have adopted ALPR technology to accumulate detailed data about individual and mass movement.[88] They are motivated to adopt surveillance technology for various reasons, such as safety, profit, and efficiency, that range from benign to unconscionably intrusive. [89] The depth of intrusion encouraged by ALPR technology is best revealed in the context of law enforcement.

---

[83] *Id.*
[84] *Id.* at 1185.
[85] *Id.*
[86] *You Are Being Tracked*, AM. C. L. UNION (July 2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/99XJ-HSXM].
[87] *See* Katz v. United States, 389 U.S. 347, 351 (1967).
[88] *See* Díaz & Levinson-Waldman, *supra* note 31.
[89] A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1720 (2015) (noting and providing examples for myriad uses for surveillance technology, including identifying criminal suspects, permitting location-based marketing, and enabling efficient design by urban planners).

Law enforcement has gravitated quickly toward the use of ALPR technology, a tendency attributable to three interrelated developments: 1) An increased need for automated processes to check/flag criminal suspects due to population increase; 2) the use of technology in lieu of real-time enforcement measures; and 3) the use of a vehicle registration plate as a unique signifier, which can generate secondary links to a "data double" of the vehicle's owner – potentially revealing individual offenses through automated cross-matching.[90] By embracing *automated* data matching, law enforcement can conduct *broader* data matching.[91] They are no longer confined to their internal independent records; they can now match data collected across multiple agencies.[92]

This section of the study addresses the various issues, and attendant privacy concerns, presented by the broad deployment of ALPR technology.

### *A. ALPR Technology Encourages Overly Broad Surveillance Practices*

The scale at which ALPR technology is deployed presents significant privacy concerns. ALPR technology enables a uniquely intrusive type of surveillance: "public camera surveillance with population analysis."[93] To achieve this aim, ALPRs capture and store massive quantities of data, but the majority of this data involves individuals suspected of *no* criminal activity.[94] As an example, a 2012 ACLU analysis of license-plate scans in Maryland revealed that for every 1 million plates scanned, only 47 were possibly linked to "serious crimes."[95] This paltry rate of return – only 0.000047% of all scans having the potential to uncover "serious crimes" – suggests that the significant attendant privacy invasions must be more carefully evaluated.[96]

---

[90] Ian Warren et al., *When the Profile Becomes the Population: Examining Privacy Governance and Road Traffic Surveillance in Canada and Australia*, 25 CURRENT ISSUES CRIM. JUST. 565, 568 (2013).
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] AM. C. L. UNION, *supra* note 86, at 7.
[95] *Id.* at 14.
[96] *Id.*

Law enforcement uses ALPR data in two ways: reactive purposes and analytic purposes.[97] "Reactive" uses are when law enforcement officials obtain license plate information and check it against existing databases.[98] These uses typically trigger few to no privacy concerns.[99] "Analytic" uses, however, impact privacy much more significantly. Here, law enforcement mines the existing databases for license plate information to further an existing investigation or, more concerningly, to commence an unrelated investigation.[100]

Through computer analytics, law enforcement agencies can sort through this data not just to locate existing suspects but to identify potential *future* crimes.[101] In addition to the location of a specific car at a specific time, it is possible to infer detailed information about individual habits and addresses.[102] In the context of GPS tracking, the U.S. Court of Appeals for the D.C. Circuit discussed the types of personally identifiable information (PII) that can be ascertained:

> A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving

---

[97] KEITH GIERLACK ET AL., LICENSE PLATE READERS FOR LAW ENFORCEMENT: OPPORTUNITIES AND OBSTACLES 8 (RAND, 2014).
[98] *Id.*
[99] Koops et al., *supra* note 38, at 672 (for example, in the Netherlands, law enforcement can only use ALPR technology in reactive ways. "[I]t does not involve systematic *following* of a person. ALPR might be based on Article 3 of the Police Act of 2012 if the police are looking for particular cars with known license plate numbers from a reference database, which are automatically matched with the plate numbers of cars passing by, and the photograph and plate number of an observed car is recorded only if a match is found.").
[100] GIERLACK ET AL., *supra* note 97, at 8 (for instance, in Germany, an analytic approach is used in "in cases of offenses of substantial significance and where other means of establishing the facts or determining the perpetrator's whereabouts would offer much less prospect of success or be much more difficult."); Koops et al., *supra* note 38, at 672 (the use of ALPR in Germany requires authorization from a judge though, which is different than in the U.S. and the U.K.).
[101] Joh, *supra* note 21, at 16-17.
[102] Cyrus Farivar, *We Know Where You've Been: ARS Acquires 4.6M License Plate Scans from the Cops*, ARS TECHNICA (Mar. 24, 2015, 9:00 AM), https://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/ [https://perma.cc/7U2D-DDRW].

> medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.[103]

Computer analytics also enable law enforcement to parse the locational data for suspicious activities.[104] Combining this data with social network analysis can reveal connections between individuals that could be impossible to deduce otherwise.[105] The data can also be aggregated and analyzed to unveil "crime patterns and trends."[106]

The benefit to law enforcement from ALPR technology is obvious. But the attendant privacy concerns are arguably paramount. The balance is especially critical when considering how the nature of ALPR technology – which can be deployed easily and broadly to aid in the investigation process – encourages truly abusive practices.

### *B. ALPR Technology Encourages Abusive Surveillance Practices*

ALPR technology, by its nature, encourages abusive investigation practices that threaten privacy. ALPR technology has impacted the "surveillance discretion" of officers, defined as "when, how, and whether the police may target a person or persons in the initial phases of governmental investigation."[107] The limits of surveillance discretion, however, are salient given the uniquely invasive nature of ALPR technology.

ALPR technology fundamentally changes how law enforcement decides to target individuals for further surveillance. It warrants further analysis because "[b]y allowing the identification of large numbers of suspicious activities and people by sifting through large quantities of digitized data, big data expands the surveillance discretion of the

---

[103] AM. C.L. UNION, *supra* note 94, at 8 (citing United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010)).
[104] *Id.* at 7.
[105] Joh, *supra* note 21, at 25; GIERLACK ET AL., *supra* note 97, at 10 (discussing the information that analytic uses can uncover).
[106] GIERLACK ET AL., *supra* note 97, at 10.
[107] Joh, *supra* note 21, at 15.

police."[108] The Supreme Court has repeatedly held that law enforcement has significant discretion when determining whether to investigate an individual.[109] But ALPRs entail a very real possibility of law enforcement overreach. The traditional deference afforded to law enforcement should be re-evaluated given these pressing privacy concerns.

Law enforcement has used a variety of practices – some highly intrusive – to track criminal suspects.[110] Using this technology, police can not only track both suspects of, and witnesses to, a crime, they can track "objects, such as cell-phones or containers; and they can collect data about movements in the past, or track movements in real time."[111]

Some law enforcement precincts use the concept of "hit rates" to identify so-called "hot spots" or "hot times" to help them identify where and when to deploy ALPR technology.[112] For example, if a fixed ALPR camera had several flagged "hits" from license plates with drivers with traffic violations, this might identify a hot spot for law enforcement to mobilize an ALPR camera attached to a squad car. Legal researchers have decried this practice, noting that it can lead to racial and other types of profiling based on the geography of different jurisdictions.[113]

ALPR data collection is not generally a cause of *direct* discrimination by law enforcement, but it can lead to indirect or concealed discrimination.[114] With indirect discrimination, certain facially neutral

---

[108] *Id.* at 19.
[109] *See* Anna Lvovsky, *The Judicial Presumption of Police Expertise*, 130 HARV. L. REV. 1995 (2017) (specifically, since *Terry v. Ohio*, the Supreme Court has urged the courts to give "due weight to inferences drawn by policemen 'in light of [their] experience" and presumed expertise (citing Terry v. Ohio, 382 U.S. 1, 27 (1968))). This has expanded to include investigatory discretion as well. *Id.* at 1997.
[110] Koops et al., *supra* note 38, at 638.
[111] *Id.*
[112] Warren et al., *supra* note 90, at 576-77.
[113] *Id.* at 577 (characterizing the practice as "ill- conceived").
[114] MANDANA ZARREHPARVAR, *A Nondiscriminatory Information Society*, *in* HUMAN RIGHTS IN THE GLOBAL INFORMATION SOCIETY, 222 (2006). Direct discrimination is when "one person is treated less favorably than another is, has been, or would be treated in a comparable situation on prohibited grounds." *Id.*

data collection practices may actually target and disadvantage particular groups of people.[115] Law enforcement may deploy ALPRs in neighborhoods dubbed "high risk," but in practice, this leads to indirect discrimination.[116] So-called "high-risk" areas are disproportionately home to minority groups and/or individuals in lower socio-economic spheres.[117] For example, in Birmingham, U.K., law enforcement used ALPR technology to monitory the daily movements of a mostly Muslim community.[118] The nominally "neutral" data collection practices may serve as a cover for ingrained discrimination.[119]

There are some counter arguments that broad use of surveillance technologies may actually reduce racial profiling.[120] Because indiscriminate observational data removes individual police officer discretion in running plates, ALPR systems might correct implicit racial biases held by police officers.[121] However, the technology can still be abused by racially biased police officers. To illustrate, there is anecdotal evidence that individual officers have looked up license places parked near a LGBTQ bar in order to blackmail the car's owners.[122] Given the potential for surveillance abuse, ALPR technology should be viewed with healthy skepticism and with an eye toward preventing invasive practices.

### *C. ALPR Data Storage Practices Impact Personal Privacy*

The storage of ALPR data compounds the privacy issues outlined above. Information about every license plate – even those for vehicles not associated with crimes – is captured and stored in ALPR databases.[123] Some laws regulate the collection and retention of data,

---

[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 286 (2011).
[119] *Id.* at 299.
[120] *Id.* at 298.
[121] *Id.*
[122] Friedman & Janszky, *supra* note 25, at 19.
[123] GIERLACK ET AL., *supra* note 97, at 2.

but many jurisdictions lack laws providing clear guidelines or adequate legal recourse for inadequate data security practices.[124] Many states in the U.S. lack statutory restrictions; absent these, ALPR data could theoretically be stored and used indefinitely. Even in states with statutory restrictions, however, there is wide variance in terms of whether data storage is addressed.[125] Additionally, the lack of comprehensive guidelines to data storage and retention in a world that is increasingly physically mobile, presents barriers to data management.

## III. U.S. AND U.K. RESPONSE TO ALPR TECHNOLOGY AND PRIVACY

In both the U.S. and the U.K., governmental entities have proposed regulations aimed at protecting individuals' privacy and curbing the potential for law enforcement abuse of ALPR technology.[126] The approaches they have adopted, however, are different. This section of the study evaluates statutes that have been passed in sixteen U.S. states, non-binding federal guidelines, and nationally binding guidelines adopted in the U.K.

### *A. The U.S. Response to ALPR Use*

The U.S. has responded to ALPR use by developing piecemeal legislation that fails to protect privacy adequately. [127] Some government agencies have wholly neglected to adopt policies that safeguard individual privacy, while the policies that *have* been adopted are wildly varied.[128] Overall, existing U.S. policies demonstrate a far less consumer-centric approach to personal data management than that in the U.K. Individuals in the U.S. are provided with very little knowledge of – let alone control over – how their personal data is collected,

[124] *Id.*
[125] *Id.*
[126] Díaz & Levinson-Waldman, *supra* note 31.
[127] Bayley, *supra* note 33.
[128] *Id.*

secured, and shared.[129] While these privacy policies may passively inform individuals that their data is being collected, current U.S. law provides no federal safeguards explicating how that data may be utilized or outlining mechanisms for access to and erasure of that data.[130] The U.S. approach, as argued in this study, is untenable.

### *B. The U.S. Judicial Approach to ALPR Regulation*

The Fourth Amendment to the U.S. Constitution safeguards the right to be free from "unreasonable searches and seizures" by the government.[131] Historically, courts considered these issues in the context of physical trespass on personal property.[132] This analysis extended to electronic invasions of privacy starting in 1967 when the Supreme Court decided *Katz v. United States*.[133] In *Katz*, law enforcement agents used microphones to eavesdrop on telephone calls the defendant made in a public phone booth.[134] The Supreme Court determined that Katz had a "reasonable expectation of privacy" and that, therefore, this search violated Katz's Fourth Amendment rights.[135]

There has also been concern that *Katz's* focus on expectations is particularly troubling in the context of new technologies. The Seventh Circuit indicated that courts' interpretation of *Katz* "may eventually afford the government ever-wider latitude over the most sophisticated, intrusive, and all-knowing technologies with lessening constitutional constraints."[136] The court noted that the "chronicle of cameras" could

---

[129] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RSCH. CTR. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/SR6Z-YDY9].

[130] Andy Green, *Complete Guide to Privacy Laws in the U.S.*, VARONIS: INSIDE OUT SECURITY BLOG (Apr. 2, 2021), https://www.varonis.com/blog/us-privacy-laws/ [https://perma.cc/C259-G6M3].

[131] U.S. CONST. amend. IV.

[132] *The Interest Protected*, JUSTIA, https://law.justia.com/constitution/us/amendment-04/03-the-interest-protected.html [https://perma.cc/R6HX-P996].

[133] Katz v. United States, 389 U.S. 347 (1967).

[134] *Id.* at 348.

[135] *Id.* at 360.

[136] United States v. Tuggle, 4 F.4th 505, 510 (7th Cir. 2021).

reasonably expect to proliferate unfettered, which would naturally yield new Fourth Amendment concerns.[137]

Courts engaging in Fourth Amendment analysis have typically followed the same pattern in *Katz*, however: they analyze particular behaviors to determine whether they constitute a justifiable "search."[138] The collection of data via ALPRs, however, would not be a "search" triggering traditional Fourth Amendment concerns. Obtaining license-plate information for a particular vehicle would typically pose little to no privacy concerns because the license-plate information would be collected in public, and historically there has been no reasonable expectation of privacy in information made public.[139] Even if law enforcement checked the individual's license-plate information against existing "hot lists"[140] of stolen or wanted vehicles, the impact on privacy would be, at worst, negligible.[141] With respect to ALPR use, privacy issues arise not from the individualized capture of information (which would be central to the Fourth Amendment analysis), but from the bulk collection of license-plate data and how that information is retained,

---

[137] *Id.* at 527-28.

[138] *See* United States v. Knotts, 460 U.S. 276, 281 (1983) (holding that defendant had no reasonable expectation of privacy where law enforcement used a radio transmitter to track a container in his vehicle); *see also* United States v. Karo, 468 U.S. 705, 714-15, 721 (1984) (finding that law enforcement could constitutionally employ a radio transmitter to track a container on public roads but not in a private residence).

[139] *Katz*, 389 U.S. at 351 (recognizing that when individuals "knowingly expose" information to the public, they forfeit a reasonable expectation of privacy); *see* Olabisiomotosho v. City of Houston, 185 F.3d 521, 529 (5th Cir. 1999) (noting that there is no privacy interest in license plate numbers because they are "constantly open to the plain view of passersby").

[140] "Hot lists" are lists of such information as "license plate numbers related to stolen vehicle reports, active arrest warrants, AMBER alters, parolees, and known sex offenders." ROBERTS & CASANOVA, *supra* note 7, at 25-26., *quoted in* Jessica Gutierrez Alm, *The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 HAMLINE L. REV. 127, 131 (2015).

[141] *See* United States v. Ellison, 462 F.3d 557, 562 (6th Cir. 2006) (stating that "the very purpose of a license plate number . . . is to provide identifying information to law enforcement officials and others"); United States v. Diaz-Castaneda, 494 F.3d 1146, 1151 (9th Cir. 2007) ("[n]o one can reasonably think that his expectation of privacy has been violated when a police officer sees what is readily visible and uses the license plate number to verify the status of the car and its registered owner"); United States v. Walraven, 892 F.2d 972, 974 (10th Cir. 1989) ("no privacy interest exists in license plates").

used and disclosed to third parties.[142] Thus far, the courts have largely failed to catch up to societal trends post 9/11, wherein federal intelligence agencies have enlisted state and local police departments as their "eyes and ears."[143] As a part of this process, both the Department of Justice and the Department of Homeland Security have grant-in-aid programs that fund the acquisition of equipment ostensibly for technologies to aid counterterrorism and generalized law enforcement activities.[144] Additionally, many precincts have Joint Terrorism Task Forces that coordinate counterterrorism activity across various levels of government.[145] The acquisition of surveillance technology by local law enforcement, combined with gaps in federal and state legislation, have led to what is known as the "public surveillance gap," wherein mass surveillance is pervasive, but the Fourth Amendment does not offer protection against police use of surveillance in public spaces.[146]

While the Supreme Court has recently indicated a willingness to revisit some of the new issues generated by changes in technology, they have not discretely dealt with the issue of public surveillance by law enforcement. In *United States vs. Jones*, police attached a GPS tracking device to a drug suspect's car without a valid warrant and tracked his movement for twenty-eight days.[147] Justice Scalia, in the majority

---

[142] Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 ME. L. REV. 397, 435 (2014).

[143] Ira S. Rubinstein*, Privacy Localism*, 93 WASH. L. REV. 1961, 1971 (2018).

[144] *Id.* at 1971-72.

[145] *Id. See generally* Matthew C. Waxman, *National Security Federalism in the Age of Terror,* 64 STAN. L. REV. 289 (2012); Susan N. Herman, *Collapsing Spheres: Joint Terrorism Task Forces, Federalism, and the War on Terror,* 41 WILLAMETTE L. REV. 941 (2005).

[146] Rubinstein*, supra* note 143, at 1974-75. While federal electronic surveillance statues offer some protection under the Electronic Communications Privacy Act of 1986, the law and its various provisions, focus on wire taps of telephone calls. Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523. Even for protections from wiretaps, the ECPA is outdated. In a 2011 *New York Times* article, University of San Francisco Law Professor Susan Freiwald was quoted as saying "[s]ome people think Congress did a pretty good job in 1986 seeing the future, but that was before the World Wide Web . . .. The law can't be expected to keep up without amendments." Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. TIMES (Jan. 9, 2011), https://www.nytimes.com/2011/01/10/technology/10privacy.html [https://perma.cc/4FBV-RQN5]. This law merely, and inadequately, covers the use of wiretaps by law enforcement on the public. It completely does not address public surveillance by law enforcement.

[147] United States v. Jones, 565 U.S. 400, 402-03 (2012).

opinion, cited traditional trespass theory under the Fourth Amendment to rule that the physical installation of the device constituted a "search," thereby ignoring the issue of long-term GPS monitoring as a privacy issue.[148]

Two opinions by Chief Justice Roberts attempt to remedy the concerns of extending a Fourth Amendment approach grounded in traditional property theory to cases involving the use of novel and specialized technologies.[149] The decisions have decidedly different application to the issue of ALPRs, however.

The first decision, *Riley v. California* (2014), articulates the modern issues presented by modern technology: the cell phone.[150] In this case, the Supreme Court held that police could not conduct a warrantless search of a cell phone seized during an arrest due to the "immense storage capacity" of the cell phone.[151] Searching the vast quantities of information on a phone presents a significant invasion of privacy that necessitates implementing strict procedural safeguards.[152] The *Riley* decision provides authority for the position that ALPRs, which are also deployed for the bulk collection of data, should be viewed similarly.

The second decision, *Carpenter v. United States* (2018), has more limited utility.[153] In this 5-4 decision, the Court held that when law enforcement or the government access historical cell phone locational data, this constitutes a search under the Fourth Amendment.[154] That

---

[148] *Id.* at 404-09. In two separate concurrences, five of the justices specifically attempted to confront the issue of whether long-term GPS monitoring was a violation of the suspect's reasonable expectation to privacy under the *Katz* standard; both concurrences concluded that it did. *Id.* at 413-18 (Sotomayor, J., concurring); *Id.* at 418-31 (Alito, J., concurring).
[149] *See* Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 138 S. Ct. 2206 (2018).
[150] *Riley*, 573 U.S. at 373.
[151] *Id.* at 375. Chief Justice Roberts referred to the storage capacity as "one of the most notable distinguishing features of modern cell phones." According to Roberts, prior to cell phones, a physical search of a suspect by law enforcement was limited to the "physical realities" of what they carried on them, constituting only a narrow intrusion on privacy. Searching a modern phone, without a warrant, would be a much greater intrusion.
[152] *Id.*
[153] Carpenter, 138 S. Ct. 2206.
[154] *Id.* at 2220.

being said, the *Carpenter* decision rests on exceptionally narrow grounds.[155] The Court clarified that its decision was a "narrow one" that does not extend to other types of technology.[156] Specifically, the Court said that the *Carpenter* decision does not apply to "conventional surveillance techniques and tools, such as security cameras."[157] Additionally, the Supreme Court noted that the decision did not apply to "business records that might incidentally reveal location information" or "other collection techniques involving foreign affairs or national security."[158]

Scholar Ira S. Rubinstein argues that, read together, *Jones, Riley,* and *Carpenter* suggest that a line can be drawn between law enforcement engaging in broad, unrestrained surveillance aided by new technology, and a justified, more limited, approach to surveillance technology.[159] Specifically, these decisions suggest that there may be a reasonable expectation to privacy even in public places, which precludes the legality of an all-encompassing surveillance state.[160]

### *C. The U.S. Legislative Approach to ALPR Regulation*

Since the 2000s, the U.S. Congress has "largely abdicated its role in regulating online consumer privacy or modernizing electronic surveillance laws to strengthen privacy protections in the context of emerging technologies."[161] In the absence of substantive federal regulations, states have increasingly ventured to pass state-specific

---

[155] *Id.*
[156] *Id.*
[157] *Id.*
[158] *Id.* Despite the narrowness of the holding, at least one law review note argues that ALPRs should constitute a search post-*Carpenter*. See generally, Stephanie Foster, *Should the Use of Automated License Plate Readers Constitute a Search After Carpenter v. United States?*, 97 WASH. U. L. REV. 221 (2019).
[159] Rubinstein*, supra* note 143, at 1978.
[160] *Id.*
[161] *Id.* at 1963. This is a shift from the 1970s to 1990s, when the U.S. Congress passed and updated several important privacy laws. Although both Democrats and Republicans have introduced comprehensive online privacy consumer bills, none of these bills was successfully passed. *Id*. In fact, in 2000, a Stanford Law Review symposium titled "Cyberspace and Privacy: A New Legal Paradigm?" asked: "is privacy dead?" While the argument from Professor Michael Froomkin in 2000 was "no," technology has continued to aid an almost unchecked expansion of federal surveillance laws and practices. *Id*. at 1968-69.

online privacy laws.[162] This sometimes has a patchwork effect, especially with regard to the treatment of emerging technology like ALPRs.[163] Some cities and counties are also pursuing highly local privacy law and regulation, a trend called privacy localism.[164] Although very little legal research has focused on these local privacy regulations, as urban centers become increasingly data rich, a growing number of police departments rely on city guidance for the use of security cameras, facial recognition technology, dashcams, bodycams, and ALPRs.[165] In the absence of federal and state guidance, some cities have stepped into the void.[166]

In the U.S., sixteen states[167] have adopted statutes that regulate the use, retention and/or dissemination of ALPR data.[168] Bills regulating ALPRs

---

[162] *Id.* at 1963.

[163] *Id.*

[164] *Id.* at 1964.

[165] *Id.* As of 2018, more than fifteen cities have enacted surveillance ordinances disclosing the deployment and use of surveillance equipment. Some cities have also developed privacy guidelines for the use of smart city/Internet of Things data practices. Seattle and New York cities are seen as emerging leaders in privacy localism. *Id*. at 1966.

[166] *Id.* at 1966. Legal scholar Rubinstein promotes privacy localism, defined specifically as a "preference for local control of government function" as a necessary part of regulating local police surveillance activities as well as local data governance practices. *Id*. at 1967. While Rubinstein acknowledges that some skeptics express doubts about the viability of privacy localism, that federal and state pre-emption is countered by the benefit of the gaps covered by privacy localism. The authors of this piece see the benefit of local regulations *when* there is a state and federal level gap in privacy law relating to new technology, but also argue that given the *ubiquitous* nature of surveillance technology, that stronger federal guidelines should be adopted by most countries to reflect their cultural and legal norms. More succinctly put, a patchwork approach to surveillance technology does not benefit individuals being governed by them.

[167] ARK. CODE ANN. § 12-12-1801 (West 2013); CAL. VEH. CODE § 2413 (West 2011); CAL. CIV. CODE § 1798.29 (West 2020); CAL. CIV. CODE § 1798.90.5 (West 2016); COLO. REV. STAT. ANN. § 24-72-113 (West 2014); FLA. STAT. ANN. § 316.0777 (West 2019); GA. CODE ANN. § 35-1-22 (West 2018); ME. REV. STAT. ANN. tit. 29-A, § 2117-A (West 2013); MD. CODE ANN., Pub. Safety § 3-509 (West 2019); MINN. STAT. ANN. § 13.824 (West 2021); MONT. CODE ANN. § 46-5-117 (West 2017); NEB. REV. STAT. § 60-3201 (West 2018); N.H. REV. STAT. ANN. § 236:130 (West 2014); N.H. REV. STAT. ANN. § 261:75-b (West 2016); N.C. GEN. STAT. ANN. § 20-183.30 (West 2015); OKLA. STAT. ANN. tit. 47, § 7-606.1 (West 2017); TENN. CODE ANN. § 55-10-302 (West 2014); TENN. CODE ANN. § 10-7-504 (32)(A) (West 2021); UTAH CODE ANN. § 41-6a-2001 (West 2013); VT. STAT. ANN. tit. 23, § 1607 (West 2018).

[168] Colorado's statute is unusual among these sixteen because it is an open-records statute regulating the accessibility and retention of "passive surveillance records," defined to include

have been proposed in at least four more states.[169] The majority of these statutes restrict how law enforcement (or, to a lesser extent, other government agencies) can use ALPR technology.[170] Some of these statutes further exclude certain private individuals or organizations from using ALPR technology.[171] For example, Arkansas prohibits ALPR technology from being used not only by "the State of Arkansas, its agencies, and political subdivisions," but also by "an individual, partnership, corporation, or association."[172]

Broadly the state statutes included the following policies: ALPR usage restrictions, data retention, transparency, access, training, and penalties. This section of the study addresses each policy generally, before

---

still images and videos captured by a variety of recording devices, though specifically excluding toll collection cameras. COLO. REV. STAT. ANN. § 24-72-113 (West 2014). While the statute does not articulate provisions unique to ALPRs, its breadth encompasses ALPR-generated records.

[169] These states are Massachusetts (H.3564, 192nd Gen. Assemb., Reg. Sess. (Mass. 2021); H.3597, 192nd Gen. Assemb., Reg. Sess. (Mass. 2021)); New Jersey (Assemb.2384, 219 Gen. Assemb., Reg. Sess. (N.J. 2020)); New York (Assemb.00940, Gen. Assemb., Reg. Sess. (N.Y. 2021); and Pennsylvania (H.133, Gen. Assemb., Reg. Sess (Pa. 2021)).

[170] ARK. CODE ANN. § 12-12-1801 (West 2013); CAL. VEH. CODE § 2413 (West 2011); CAL. CIV. CODE § 1798.29 (West 2020); CAL. CIV. CODE § 1798.90.5 et seq. (West 2016); COLO. REV. STAT. ANN. § 24-72-113 (West 2014); FLA. STAT. ANN. § 316.0777 (West 2019); GA. CODE ANN. § 35-1-22 (West 2018); ME. REV. STAT. ANN. tit. 29-A, § 2117-A (West 2013); MD. CODE ANN., PUB. SAFETY § 3-509 (West 2019); MINN. STAT. ANN. § 13.824 (West 2021); MONT. CODE ANN. § 46-5-117 (West 2017); NEB. REV. STAT. § 60-3201 (West 2018); N.H. REV. STAT. ANN. § 236:130 (West 2014); N.H. REV. STAT. ANN. § 261:75-b (West 2016); N.C. GEN. STAT. ANN. § 20-183.30 (West 2015); OKLA. STAT. ANN. tit. 47, § 7-606.1 (West 2017); TENN. CODE ANN. § 55-10-302 (West 2014); TENN. CODE ANN. § 10-7-504 (32)(A) (West 2021); UTAH CODE ANN. § 41-6a-2001 (West 2013); VT. STAT. ANN. tit. 23, § 1607 (West 2018).

[171] ARK. CODE ANN. § 12-12-1801 (West 2013); CAL. VEH. CODE § 2413 (West 2011); CAL. CIV. CODE § 1798.29 (West 2020); CAL. CIV. CODE § 1798.90.5 (West 2016); COLO. REV. STAT. ANN. § 24-72-113 (West 2014); FLA. STAT. ANN. § 316.0777 (West 2019); GA. CODE ANN. § 35-1-22 (West 2018); ME. REV. STAT. ANN. tit. 29-A, § 2117-A (West 2013); MD. CODE ANN., PUB. SAFETY § 3-509 (West 2019); MINN. STAT. ANN.§ 13.824 (West 2021); MONT. CODE ANN. § 46-5-117 (West 2017); NEB. REV. STAT. § 60-3201 (West 2018); N.H. REV. STAT. ANN. § 236:130 (West 2014); N.H. REV. STAT. ANN. § 261:75-b (West 2016); N.C. GEN. STAT. ANN.§ 20-183.30 (West 2015); OKLA. STAT. ANN. tit. 47, § 7-606.1 (West 2017); TENN. CODE ANN. § 55-10-302 (West 2014); TENN. CODE ANN. § 10-7-504 (32)(A) (West 2021); UTAH CODE ANN. § 41-6a-2001 (West 2013); VT. STAT. ANN. tit. 23, § 1607 (West 2018).

[172] ARK. CODE ANN. § 12-12-1803(a) (West 2017).

providing deeper analysis of any unique elements that warrant individual discussion. The following table highlights the common statutory provisions and indicates which states have incorporated those elements in their statutes:

| State ALPR Policies | ALPR Usage Restrictions | Data Retention | Transparency | Access | Training | Penalties |
|---|---|---|---|---|---|---|
| Arkansas | X | X | X | X | | X |
| California | X | X | X | X | | X |
| Colorado | | X | | | | |
| Florida | | | | X | | |
| Georgia | X | X | | X | X | X |
| Maine | X | X | | | | |
| Maryland | X | | | X | X | X |
| Minnesota | X | X | X | X | | X |
| Montana | X | X | X | X | X | X |
| Nebraska | X | X | X | X | | X |
| New Hampshire | X | X | X | X | | |
| North Carolina | X | X | | X | | |
| Oklahoma | X | | | | | |
| Tennessee | | X | | X | | |
| Utah | X | X | | X | | X |
| Vermont | X | X | X | X | X | |
| **State Totals:** | 13 | 13 | 7 | 13 | 4 | 8 |

These provisions are addressed below.

### *D. ALPR Usage Restrictions*

Thirteen state statutes address, in some form, what entities can use ALPR technology.[173] Mainly, these statutes empower or guide law

[173] ARK. CODE ANN. § 12-12-1803 (West 2017) (making it illegal to for "an individual, partnership, corporation, association," or Arkansas state agencies to use ALPRs, and limiting use to law enforcement agencies and parking enforcement agencies); CAL. VEH. CODE § 2413 (West 2011) (establishing that the Department of the California Highway Patrol can create programs enabling law enforcement to use ALPR technology to combat theft); CAL. CIV. CODE § 1798.90.5 (West 2016); GA. CODE ANN. § 35-1-22 (West 2018) (addressing the use of

enforcement in the use of ALPRs.[174] Additionally, some of these statutes further delineate exactly how and when law enforcement can use this technology.[175] They occasionally restrict law enforcement use of ALPRs to specific purposes, such as protecting public safety or

---

ALPR data by law enforcement agencies); ME. REV. STAT. ANN. tit. 29-A, § 2117-A (West 2013); MD. CODE ANN., PUB. SAFETY § 3-509 (West 2019) (addressing the use of ALPRs by law enforcement); MINN. STAT. ANN. § 13.824 (West 2015) (addressing the use of ALPRs by law enforcement); MONT. CODE ANN. § 46-5-117 (West 2017) (stating that, generally, agencies or employees of the state cannot use ALPRs on a public highway); NEB. REV. STAT. ANN. § 60-3203 (West 2018) (prohibiting the use of ALPRs by governmental entities); N.H. REV. STAT. ANN. § 236:130(II) (West 2014) (generally restricting the state from surveilling individuals on public streets); N.H. REV. STAT. ANN. § 261:75-B (West 2016) (restricting ALPRs to law enforcement use); N.C. GEN. STAT. ANN. § 20-183.31 (West 2015) (addressing the use of ALPRs by law enforcement); OKLA. STAT. ANN. tit. 47, § 7-606.1 (West 2017); UTAH CODE ANN. § 41-6a-2003 (West 2013) (addressing the use of ALPRs); and VT. STAT. ANN. tit. 23, § 1607 (West 2018) (addressing the use of ALPRs by law enforcement).

[174] *See, e.g.*, ARK. CODE ANN. § 12-12-1803 (West 2017); CAL. VEH. CODE § 2413 (West 2011); CAL. CIV. CODE § 1798.90.5 (West 2016); GA. CODE ANN. § 35-1-22 (West 2018); ME. REV. STAT. ANN. tit. 29-A, § 2117-A (2013); MD. CODE ANN., PUB. SAFETY § 3-509 (West 2019); MINN. STAT. ANN. § 13.824 (West 2021); MONT. CODE ANN. § 46-5-117 (West 2017); NEB. REV. STAT. ANN. § 60-3203 (West 2018); N.H. REV. STAT. ANN. § 236.130(II) (West 2014); N.H. REV. STAT. ANN. § 261:75-B (West 2016); N.C. GEN. STAT. ANN. § 20-183.31 (West 2015); OKLA. STAT. ANN. tit. 47, § 7-606.1 (West 2017); UTAH CODE ANN. § 41-6A-2003 (West 2020); and VT. STAT. ANN. tit. 23, § 1607 (West 2018).

[175] ARK. CODE ANN. § 12-12-1801-1808 (West 2013) (providing limited exceptions for law enforcement agencies (including for conducting ongoing investigations), parking enforcement entities, the Arkansas Highway Police Division of the DOT (to verify registration and collect compliance data), and for controlling access to secure areas); GA. CODE ANN. § 35-1-22(b) (West 2018) (stating that law enforcement can collect captured license plate data); ME. REV. STAT. ANN. tit. 29-A, § 2117-A(3) (2013) (limiting ALPR use to the Department of Transportation for public safety and infrastructure purposes; the Department of Public Safety for commercial motor vehicle screening and inspection; and law enforcement agencies for criminal investigations); MD. CODE ANN., PUB. SAFETY § 3-509(a)(8)-(b)(1) (West 2019) (limiting ALPR technology by law enforcement to "limited purposes," defined as "the investigation, detection, or analysis of a crime or a violation of the Maryland vehicle laws or the operation of terrorist or missing or endangered person searches or alerts."); MINN. STAT. ANN. § 13.824(c)-(d) (West 2015) (outlining the specific purposes for which ALPRs can be used); MONT. CODE ANN. § 46-5-117(1) (West 2017) (generally restricting agencies or state employees from using ALPRs on a public highway); N.H. REV. STAT. ANN. § 236:130 (2014) (enabling public surveillance for various purposes, including the pursuance of a criminal investigation or for toll collection); N.H. REV. STAT. ANN. § 261:75-b (2016) (limiting law enforcement ALPR use to identifying various vehicles, including stolen vehicles and vehicles associated with missing persons); N.C. GEN. STAT. § 20-183.30-32 (West 2015); OKLA. STAT. ANN. tit. 47, § 7-606.1 (West 2017); UTAH CODE ANN. § 41-6a-2003 (West 2013) (noting that governmental entities generally cannot use ALPRs); VT. STAT. ANN. tit. 23, § 1607, 1608 (West 2018).

conducting ongoing criminal investigations.[176] These lists of "restrictions" can be exceptionally lengthy, such as in Nebraska, which enables law enforcement to use ALPRs for numerous reasons, including identifying outstanding parking or traffic violations, locating unregistered or stolen vehicles, or furthering ongoing criminal investigations.[177]

Some states have unique usage provisions.[178] California, for example, contains a provision specifically addressing the use of ALPR technology by the California Highway Patrol (CHP).[179] The CHP can make the data available to law enforcement officers, who are restricted from using it unless they are attempting to locate a vehicle or person "when either are reasonably suspected of being involved in the commission of a public offense."[180] And in Vermont, law enforcement can use ALPRs, but only for "legitimate" purposes, including establishing a person's defense to criminal charges.[181] The law specifically excludes parking enforcement and traffic violations from the definition of "legitimate" purposes.[182]

Three states – Oklahoma, Utah, and Minnesota – warrant further discussion. Oklahoma's statute governing ALPR use contains exceptionally narrow protections for the public.[183] The statute limits the

---

[176] MONT. CODE ANN. § 46-5-117(2)(a)-(c) (West 2017) (enabling the Department of Transportation and incorporated cities and towns to use ALPRs to collect planning data or to identify a vehicle's location and plate number to enforce parking restrictions; to conduct various screening operations; and to monitor their own vehicles and equipment); NEB. REV. STAT. ANN. § 60-3203(2)(a) (West 2018) (establishing the circumstances in which law enforcement agencies may use ALPRs); N.H. REV. STAT. ANN. § 261:75-b (West 2016) (limiting law enforcement ALPR use to identifying various vehicles, including stolen vehicles and vehicles associated with missing persons; UTAH CODE ANN. § 41-6a-2003(2) (West 2013) (enabling law enforcement to use ALPRs to conduct criminal investigations and ensure compliance with laws); VT. STAT. ANN. tit. 23, § 1607(c) (West 2018) (limiting the use of ALPRs to "legitimate law enforcement purposes").
[177] NEB. REV. STAT. ANN. § 60-3203(2)(a) (West 2018).
[178] CAL. VEH. CODE § 2413 (West 2011); VT. STAT. ANN. tit. 23, §§ 1607, 1608 (West 2018).
[179] CAL.VEH. CODE § 2413 (West 2011).
[180] *Id.*
[181] VT. STAT. ANN. tit. 23, §§ 1607, 1608 (West 2018).
[182] *Id.*
[183] OKLA. STAT. ANN. tit. 47, § 7-606.1 (West 2017).

collection and use of data to law enforcement agencies for the purpose of the Uninsured Vehicle Enforcement program, which aims to detect offenses involving uninsured motorists.[184] However, the statute specifically protects the rights of individuals or agencies to use ALPRs *for any other legal purpose*.[185] So, while Oklahoma purports to safeguard individual information, those protections are exceptionally limited.

Utah's usage policies are more complicated. In Utah, law enforcement can use ALPR technology for specific limited circumstances, including conducting ongoing investigations or securing public safety.[186] However, the law also allows institutions of higher education to use ALPRs for various purposes, including law enforcement, parking enforcement and controlling access to secured areas.[187] Broad policies are also found in Nebraska, which enables ALPR use not only by law enforcement, but for parking enforcement, electronic toll collection and weigh station activities.[188]

Notably, Minnesota's statute limits ALPR data collection to: (1) license plate numbers, (2) date, time and location data, and (3) pictures of license plates, vehicles and areas immediately surrounding the vehicles.[189] ALPR data only can be matched with a particular database (Minnesota's license plate data file) and generally cannot be used to track an individual who is the subject of an active criminal investigation absent a warrant or probable cause.[190] These ALPR usage restrictions help limit the concerns regarding abusive data collection practices outlined in Section II of this study.[191]

---

[184] OKLA. STAT. ANN. tit. 47, § 7-606.1(C), (E)-(F) (West 2017).
[185] OKLA. STAT. ANN. tit. 47, § 7-606.1(G) (West 2017).
[186] UTAH CODE ANN. § 41-6a-2003 (West 2013).
[187] UTAH CODE ANN. § 41-6a-2003(2)(h) (West 2013) (universities can also use anonymized ALPR data for research purposes).
[188] NEB. REV. STAT. ANN. § 60-3203(2)(a)-(e) (West 2018).
[189] MINN. STAT. ANN. § 13.824(2)(a) (West 2015).
[190] *Id.* at § 13.824(c)-(d) (West 2015).
[191] *See* Joh *supra* note 21.

### *E. Data Retention*

Thirteen states have data retention requirements built into its statutes.[192] Generally, these policies address the length of time data can be retained.[193] Some of the state statutes provide hard deadlines for deleting data – from three minutes[194] to three years.[195]

---

[192] ARK. CODE ANN. § 12-12-1805 (West 2013); CAL. VEH. CODE § 2413 (West 2011), CAL. CIV. CODE § 1798.90.5 (West 2016); COLO. REV. STAT. ANN. § 24-72-113 (West 2014); GA. CODE ANN. § 35-1-22 (West 2018); ME. REV. STAT. ANN. tit. 29-A, § 2117-A(5) (West 2013); MONT. CODE ANN. §§ 46-5-118, 119(3) (West 2017); NEB. REV. STAT. ANN. § 60-3204 (West 2018); N.H. REV. STAT. ANN. § 261:75-b(VIII) (West 2016); N.C. GEN. STAT. ANN. § 20-183.32 (West 2015); TENN. CODE ANN. § 55-10-302(b)(1) (West 2014); UTAH CODE ANN. § 41-6a-2004 (West 2013); VT. STAT. ANN. tit. 23, § 1607(d) (West 2018).

[193] ARK. CODE ANN. § 12-12-1804 (West 2013) (limiting the retention of ALPR data to 150 days); CAL. VEH. CODE § 2413 (West 2011) (providing that the California Highway Patrol can only retain data for 60 days unless the data is being used as evidence or is the subject of a felony investigation); COLO. REV. STAT. ANN. § 24-72-113 (West 2014) (limiting retention to three years and requiring that specific notice of retention be given after one year); GA. CODE ANN. § 35-1-22 (West 2018) (restricting retention to 30 months, unless the data is being retained for a toll violation or law enforcement purpose); ME. REV. STAT. ANN. tit. 29-A, § 2117-A(5) (West 2013) (generally limiting retention to 21 days); MINN. STAT. ANN. § 13.824(3) (West 2015) (requiring most data to be destroyed within 60 days from collection); MONT. CODE ANN. § 46-5-118 (West 2017) (limiting data retention to 90 days); MONT. CODE ANN. § 46-5-119(3) (West 2017) (limiting ALPR database information to "the time minimally necessary, but no more than 18 months); NEB. REV. STAT. ANN. § 60-3204 (West 2018) (generally limiting retention to 180 days); N.H. REV. STAT. ANN. § 261:75-b(VIII) (West 2016) (requiring that data be purged from the system within three minutes of capture, unless the license plate number resulted in an arrest, citation or taking someone into protective custody, or if the ALPR system identified a vehicle subject to a missing or wanted person broadcast); N.C. GEN. STAT. ANN. § 20-183.32 (West 2015) (limiting retention to 90 days, except in specified circumstances); TENN. CODE ANN. § 55-10-302(b)(1) (West 2014) (limiting retention to 90 days - unless it is part of an investigation - and requiring the data be destroyed afterwards); UTAH CODE ANN. § 41-6a-2004(1)(c) (West 2013) (establishing a general 9-month retention limit); VT. STAT. ANN. tit. 23, § 1607(d) (West 2018) (establishing an 18-month retention limit, with statutory exceptions). Florida's statute merely states that a retention schedule must be established by the Department of State in consultation with the Department of Law Enforcement, but it does not include any hard guidelines for retention. FLA. STAT. ANN. § 316.0778(2) (West 2014).

[194] N.H. REV. STAT. ANN. § 261:75-b(VIII) (West 2016) (stating that records of license plates must be "purged from the system within 3 minutes of their capture in such a manner that they are destroyed and not recoverable, unless an alarm resulted in an arrest, a citation, or protective custody, or identified a vehicle that was the subject of a missing person or wanted broadcast.").

[195] COLO. REV. STAT. ANN. § 24-72-113 (West 2014) (requiring that still images or video captured by passive surveillance be deleted within three years).

Within this subset of statutes, some states build in exceptions depending on the specific information being retained.[196] Primarily, the statutes recognize retention extensions when the data is being used as evidence, is subject to a criminal investigation,[197] or is the subject of a preservation request or search warrant.[198]

Some statutes with unique provisions include Minnesota and Tennessee. In Minnesota, which requires most ALPR data to be destroyed within 60 days,[199] there is a general prohibition on the creation of a central state repository of ALPR data.[200] Tennessee's statute is also unusual because it only restricts data retention – not data gathering – by government agencies.[201] So, in Tennessee, there is no real limitation on how data can be captured and for what purpose it may be captured.

### *F. Transparency*

Seven states have statutory provisions encouraging transparency in ALPR use.[202] These provisions include explicitly requiring ALPR policies to be in writing and publicly available[203] as well as including requirements that any privacy practices -- and notice requirements --

---

[196] *See, e.g.*, CAL. VEH. CODE § 2413(b) (West 2021) (extending the 60-day limitation); NEB. REV. STAT. ANN. § 60-3204(1) (West 2018) (extending the 180-day limit).

[197] *Id.*

[198] MONT. CODE ANN. § 46-5-118(1)-(2) (West 2017) (extending the 90-day retention timeline); NEB. REV. STAT. ANN. § 60-3204(1) (West 2018) (extending the 180-day limit); VT. STAT. ANN. tit. 23, § 1608 (West 2018) (recognizing an extension of up to 90 days due to a preservation request); VT. STAT. ANN. tit. 23, § 1607(b) (West 2018). Notably, Montana limits its retention requirement to data obtained for law enforcement or criminal justice purposes. MONT. CODE ANN. § 46-5-117(2)(d)(iii) (West 2017). It also mandates the destruction of ALPR data within one year unless an additional preservation request is filed, which restarts the timeline. MONT. CODE ANN. § 46-5-118(4) (West 2017).

[199] MINN. STAT. ANN. § 13.824(2)(a) (West 2015).

[200] MINN. STAT. ANN. § 13.824(2)(c) (West 2015).

[201] TENN. CODE ANN. § 55-10-302(b) (West 2014).

[202] ARK. CODE. ANN. § 12-12-1805 (West 2013); CAL.VEH. CODE § 2413 (West 2021); MINN. STAT. ANN. § 626.8472 (West 2015); MONT. CODE ANN. § 46-5-117 (West 2017); NEB. REV. STAT. ANN. § 60-3206 (West 2018); N.H. REV. STAT. ANN. § 261:75-b(X) (West 2016); VT. STAT. ANN. tit. 23, § 1607(e) (West 2018).

[203] MINN. STAT. ANN. § 626.8472 (West 2015); MONT. CODE ANN. § 46-5-117(d) (West 2017) (requiring state and local law enforcement agencies to put ALPR policies in writing *and publicize them* before adopting ALPR technology).

also be in writing;[204] or mandating disclosure of data security breaches.[205]

Other statutes have built-in protections for preserving data and preparing it for public view -- enabling the public to serve as a "check" on the efficacy and ethics of ALPR collection practices.[206] These protections include creating a publicly viewable log of ALPR use,[207] requiring statistical data to be compiled and reviewed in a format suitable for public review,[208] and establishing procedures for a routine ALPR data audit viewable to the public.[209]

Some states include reporting guidelines in the statutes. California requires the Department of the California Highway Patrol to provide the Legislature with detailed ALPR data as part of its annual automobile theft report.[210] This data includes information about how many disclosures were made, the agencies to whom disclosures were made,

---

[204] CAL. CIV. CODE § 1798.90.51 (West 2016) (requiring ALPR operators to implement usage and privacy policies and detailing the information that must be included in the policies); NEB. REV. STAT. ANN. § 60-3206 (West 2018) (requiring ALPR policies, including privacy practices, to be in writing and posted on the relevant governmental entity web site).
[205] CAL. CIV. CODE § 1798.29 (West 2021) (requiring agencies maintaining computerized data, including "personal information" in ALPR data, to promptly notify individuals of data breaches, and providing language to include in the notification).
[206] *See, e.g.*, MINN. STAT. ANN. § 13.824(5) (West 2015) (mandating the creation of a publicly viewable log detailing the use of ALPRs).
[207] *Id.*
[208] ARK. CODE ANN. § 12-12-1805(a)(1)-(b) (West 2013) (requiring the compilation of ALPR data every six months, including how many license plates were scanned; the names of the lists these plates were checked against; the number of matches made; the number of matches that were found to be benign; and the number of matches that led to an arrest and/or prosecution); NEB. REV. STAT. ANN. § 60-3206(3) (West 2018) (requiring a publicly posted annual report on ALPR usage and practices for the Nebraska Commission on Law Enforcement and Criminal Justice).
[209] MINN. STAT. ANN. § 13.824(6) (West 2015) (establishing an outline for a biennial audit of ALPR data); MONT. CODE ANN. § 46-5-117(d)(ii) (West 2017) (requiring an audit, at least once per year, of ALPR system use and effectiveness, which is to be reported to the head of the law enforcement agency using the ALPR system); N.H. REV. STAT. ANN. § 261:75-b(X-XI) (West 2016) (establishing audit procedures to ensure compliance with the ALPR statute and to investigate complaints of ALPR misuse); VT. STAT. ANN. tit. 23, § 1607(e) (West 2018) (requiring the establishment of a review process to ensure compliance, with results reported annually to the Senate and House Committees on Judiciary and Transportation).
[210] CAL. VEH. CODE § 2413 (West 2021).

the reasons disclosures were made, and any policy changes impacting privacy.[211] Likewise, Maryland details the procedures that must be followed in creating an annual ALPR data report prepared for the Senate Judicial Proceedings Committee, House Judiciary Committee, and Legislative Policy Committee.[212] This report enables scrutiny of the collection of ALPR data. It includes detailed information including the number of ALPR units in operation, the number of hits, and the number of records retained on the ALPR database.[213]

### *G. Access*

Thirteen states address, in some capacity, whether and how ALPR data can be shared with third parties.[214] Ordinarily, these statutes enable fairly unrestricted trade of ALPR information among law enforcement agencies or for law enforcement purposes.[215] Many of these statutes,

---

[211] CAL. VEH. CODE § 2413(e) (West 2021).
[212] MD. CODE ANN., PUB. SAFETY § 3-509(e) (West 2019).
[213] *Id.*
[214] ARK. CODE. ANN. § 12-12-1806 (West 2013); CAL. VEH. CODE § 2413 (West 2011); FLA. STAT. ANN. § 316.0777 (West 2019); GA. CODE ANN. § 35-1-22 (West 2018); MD. CODE ANN., PUB. SAFETY § 3-509(d) (West 2019); MINN. STAT. ANN. § 13.824(4) (West 2015); NEB. REV. STAT. ANN. § 60-3205 (West 2018); N.H. REV. STAT. ANN. § 261:75-b (West 2016); N.C. GEN. STAT. ANN. § 20-183.31 (West 2015); TENN. CODE ANN. § 10-7-504 (32)(A) (West 2021); UTAH CODE ANN. § 41-6a-2004 (West 2013); VT. STAT. ANN. tit. 23, § 1607(c) (West 2018).
[215] *See* ARK. CODE ANN. § 12-12-1804(d)(2) (West 2013) (allowing data to be shared with other law enforcement agencies when evidence of an offense is uncovered); CAL. VEH. CODE § 2413(c) (West 2021) (restricting the Department of the California Highway Patrol from sharing ALPR data to "an agency that is not a law enforcement agency or an individual who is not a law enforcement officer"); FLA. STAT. ANN. § 316.0777 (West 2019) (stating that ALPR data can be disclosed to the individual and to a criminal justice agency in pursuance of official duties); GA. CODE ANN. § 35-1-22(c) (West 2018) (stating that law enforcement agencies can share ALPR data with other law enforcement agencies for law enforcement purposes); MINN. STAT. ANN. § 13.824(4) (West 2015) (outlining guidelines for sharing ALPR data among law enforcement agencies); MONT. CODE ANN. § 46-5-118(3) (West 2017) (outlining the specific procedures required for sharing ALPR data with law enforcement agencies); N.H. REV. STAT. ANN. § 261:75-b (West 2016) (enabling the transmission of ALPR data for law enforcement investigation and prosecution purposes); N.C. GEN. STAT. ANN. § 20-183.32(e) (West 2015) (stating that ALPR data can only be disclosed for legitimate law enforcement purposes pursuant to an agency's written request); VT. STAT. ANN. tit. 23, § 1607(c) (West 2018) (establishing guidelines for the transmission of ALPR data, including historical data, for law enforcement purposes).

however, restrict law enforcement from selling or sharing ALPR data with other third parties.[216]

The statutes permitting data sharing tend to be narrowly drawn. For example, California allows the disclosure of ALPR data to certain public agencies, but only in limited circumstances permitted by law.[217] Other states recognize regulatory compliance requirements and attendant disclosure obligations in their statutes.[218] Maine, for instance, enables law enforcement to share commercial motor vehicle screening data with the Federal Motor Carrier Safety Administration for regulatory compliance, and aggregated, non-personally-identifiable ALPR data with the public.[219]

Some states recognize other legal obligations to disclose this data, such as pursuant to court order.[220] For example, Nebraska recognizes the propriety of disclosure when necessary (1) pursuant to court order, (2) to the parties in a criminal or civil action, (3) for administrative reasons,

---

[216] ARK. CODE ANN. § 12-12-1804(d)(1) (West 2013) (stating that law enforcement agencies cannot "sell, trade, or exchange captured plate data for any purpose"); CAL. VEH. CODE § 2413(c) (West 2021) (restricting the California Highway Patrol from selling ALPR data for any reason or providing the data to non-law enforcement parties); MINN. STAT. ANN. § 13.824(4)(c) (West 2015) (prohibiting the transmission of ALPR data unrelated to active criminal investigations to third parties unless explicitly authorized by law); MONT. CODE ANN. § 46-5-118(7) (West 2017) (stating that law enforcement ALPR data cannot be sold, generally); UTAH CODE ANN. § 41-6a-2004(2) (West 2013) (prohibiting the sale or sharing of ALPR data to third parties, except for limited purposes established by statute).

[217] CAL. CIV. CODE § 1798.90.55 (West 2021). The statute explicitly notes that data hosting or towing services do not constitute the sharing of ALPR information.

[218] ME. REV. STAT. ANN. tit. 29-A, § 2117-A(4) (West 2013) (requiring the sharing of commercial motor vehicle screening data with the Federal Motor Carrier Safety Administration for regulatory compliance); MD. CODE ANN., PUB. SAFETY § 3-509(e) (West 2019) (detailing procedures for creating an annual ALPR data report prepared for the Senate Judicial Proceedings Committee, House Judiciary Committee and Legislative Policy Committee).

[219] ME. REV. STAT. ANN. tit. 29-A, § 2117-A(4) (West 2013).

[220] UTAH CODE ANN. § 41-6a-2005(2)(a) (West 2014) (recognizing that ALPR data may be disclosed upon court order); ARK. CODE ANN. § 12-12-1806 (West 2013). Arkansas law contains a unique provision that bears further discussion. It states that ALPR data is inadmissible as evidence in "any trial, hearing, or other proceeding before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the state" if that disclosure would violate Arkansas' Automated License Plate Reader System Act.

(4) to inform the public of an emergency, or (5) in connection with a missing person.[221] However, neither the ALPR data nor evidence derived from that data is admissible if it otherwise violates the Nebraska ALPR Privacy Act.[222]

Some states also include provisions establishing broad public records exemptions for ALPR data.[223] These provisions specifically indicate that ALPR data is not subject to public disclosure.[224] These policies stand in direct opposition to those adopted by Arkansas or Montana, for example, which specifically categorize ALPR data as discoverable public records.[225]

### *H. Training Requirements*

Four states – Georgia, Maryland, Montana, and Vermont – have incorporated language regarding ALPR systems training into their statutes.[226] Generally, these policies are broad and vague.[227]

---

[221] NEB. REV. STAT. ANN. § 60-3205(2) (West 2018).
[222] NEB. REV. STAT. ANN. § 60-3207 (West 2018).
[223] FLA. STAT. ANN. § 316.0777 (West 2019) (stating that ALPR records including personally identifying information are exempt from public records requests); GA. CODE ANN. § 35-1-22(f) (West 2018); MD. CODE ANN., PUB. SAFETY § 3-509(d) (West 2019) (stating that ALPR data is excluded from the Maryland Public Information Act); MONT. CODE ANN. §§ 46-5-118(5), 46-5-119 (West 2017) (broadly prohibiting public disclosure of ALPR information); NEB. REV. STAT. ANN. § 60-3209 (West 2018) (excluding ALPR data from public records disclosure requirements); N.C. GEN. STAT. ANN. § 20-183.32(e) (West 2015) (excluding ALPR from the definition of public record); TENN. CODE ANN. § 10-7-504 (32)(A) (West 2021) (stating that ALPR data is confidential and not open for public inspection).
[224] FLA. STAT. ANN. § 316.0777 (West 2019); GA. CODE ANN. § 35-1-22(f) (West 2018); MD. CODE ANN., PUB. SAFETY § 3-509(d) (West 2019); MONT. CODE ANN. §§ 46-5-118(5), 46-5-119 (West 2017); NEB. REV. STAT. ANN. § 60-3209 (West 2018); N.C. GEN. STAT. ANN. § 20-183.32(e) (West 2015); TENN. CODE ANN. § 10-7-504 (32)(A) (West 2021).
[225] ARK. CODE ANN. § 12-12-1808 (West 2011) (categorizing ALPR practice and usage data as public records under FOIA).
[226] GA. CODE ANN. § 35-1-22(e) (West 2018); MD. CODE ANN., PUB. SAFETY § 3-509(c)(2)(iii) (West 2019); MONT. CODE ANN. § 46-5-117(d)(i)(D) (West 2017); VT. STAT. ANN. tit. 23, § 1607(b) (West 2018).
[227]GA. CODE ANN. § 35-1-22(e) (West 2018); MD. CODE ANN., PUB. SAFETY § 3-509(c)(2)(iii) (West 2019); MONT. CODE ANN. § 46-5-117(d)(i)(D) (West 2017); VT. STAT. ANN. tit. 23, § 1607(b) (West 2018).

Georgia's ALPR statute declines to identify the requirements of the mandated training, but it requires law enforcement agencies to maintain policies "including but not limited to . . . the training of law enforcement officers in the use of captured license plate data. . . ."[228] Similarly, Maryland broadly directs law enforcement agencies to adopt procedures to ensure personnel are "adequately screened and trained."[229] Montana incorporates broad language requiring ALPR training, and clearly defined procedures, before ALPR technology can be adopted for law enforcement use.[230]

Though still lacking detail, Vermont has most specific training requirement. Under Vermont law, law enforcement officers must obtain certification in ALPR operation through the Vermont Criminal Justice Training Council.[231]

### *I. Penalties*

Eight states include penalty provisions – whether civil, criminal, or both – in their ALPR statutes.[232] These States differ regarding the penalties for ALPR violations. This section outlines some of the statutory penalties.

Typically the ALPR statutes provide civil relief in the form of actual damages.[233] Sometimes the statutes provide relief in the form of punitive damages and attorney's fees.[234] Individuals harmed under the California ALPR statute, for example, are entitled to actual damages (no less than liquidated damages of $2,500); they may also receive punitive damages for willful or reckless disregard for the law, attorney's fees,

---

[228] GA. CODE ANN. § 35-1-22(e) (West 2018).
[229] MD. CODE ANN., PUB. SAFETY § 3-509(c)(2)(iii) (West 2019).
[230] MONT. CODE ANN. § 46-5-117(d)(i)(D) (West 2017).
[231] VT. STAT. ANN. tit. 23, § 1607(b) (West 2018).
[232] ARK. CODE ANN. § 12-12-1807 (West 2013); CAL. CIV. CODE § 1798.90.54 (West 2021); GA. CODE ANN. § 35-1-22(d)(1) (West 2018); MD. CODE ANN., PUB. SAFETY § 3-509(b)(1) (West 2019); MINN. STAT. ANN. § 626.8472 (West 2015); MONT. CODE ANN. § 46-5-117(3) (establishing penalties for public employees or public officers who violate the ALPR statute); NEB. REV. STAT. ANN. § 60-3208 (West 2018); UTAH CODE ANN. § 41-6a-2006 (West 2013).
[233] ARK. CODE ANN. § 12-12-1807 (West 2013); CAL. CIV. CODE § 1798.90.54 (West 2021); NEB. REV. STAT. ANN. § 60-3208 (West 2018).
[234] CAL. CIV. CODE § 1798.90.54 (West 2021); NEB. REV. STAT. ANN. § 60-3208 (West 2018).

and other appropriate equitable relief.[235] In Nebraska, an individual violating the ALPR statute is liable for damages that "proximately cause injury to the business, person, or reputation of another individual or entity."[236]

Some states have incorporated criminal penalties that arguably encourage modest, targeted data collection practices. In Maryland, violating the ALPR usage restriction provision is punishable by imprisonment for up to one year or a fine of up to $10,000, or both.[237] Georgia also has onerous penalties. Obtaining, or attempting to obtain, law enforcement ALPR data for a reason other than law enforcement constitutes a "misdemeanor of a high and aggravated nature."[238] Similarly, Minnesota characterizes the unauthorized access of ALPR data as a misdemeanor,[239] and Utah classifies any violation of its ALPR statute as a Class B misdemeanor.[240] Furthermore, public employees who access this data without permission are subject to suspension or dismissal.[241]

### *J. The U.K. Response to ALPR Use*

The U.K.'s recent approach to ALPR technology has been shaped in part by the European Union's General Data Protection Regulation, enacted in 2018.[242] This regulation has intensified the focus on consent

---

[235] CAL. CIV. CODE § 1798.90.54 (West 2021).
[236] NEB. REV. STAT. ANN. § 60-3208 (West 2018).
[237] MD. CODE ANN., PUB. SAFETY § 3-509(b)(2) (West 2019).
[238] GA. CODE ANN. § 35-1-22(d)(1) (West 2018).
[239] MINN. STAT. ANN. § 626.8472 (West 2015) (incorporating criminal penalties under MINN. STAT. ANN. § 13.09 (West 2015)).
[240] UTAH CODE ANN. § 41-6a-2006 (West 2013).
[241] MINN. STAT. ANN. § 626.8472 (West 2015) (incorporating penalties for unauthorized public employee access under MINN. STAT. ANN. § 13.09 (West 2015)).
[242] *GDPR Compliance for ANPR*, PLATE RECOGNIZER, https://platerecognizer.com/gdpr-compliance-for-anpr/?utm_source=help&utm_medium=website [https://perma.cc/8S8V-HW37]. The General Data Protection Regulation concentrates on the transfer of personal data outside of the EU and the EEA (European Economic Area). According to the GDPR, individuals retain proactive control over how their personal data is collected and shared by businesses. As a result, data controllers must disclose when data collection occurs, declare the purpose for the data collection and processing, and state how long the data will be retained for and if/how it might be shared. As a part of their data management responsibilities, businesses

and privacy issues in EU countries and economic areas, including the U.K.[243]

As discussed previously in this study, license plate information falls in a legal grey area.[244] While the *intent* of regulations like the GDPR is to limit the non-consensual collection of personal data, license plate information is not always explicitly addressed. For example, under the EU's explanation of GDPR compliance, "any information" is read broadly.[245] It is intended to include both objective or subjective information about a person, and it is not limited to any specific format.[246] This information also arguably includes indirect identifiers, where "you cannot identify an individual through the information you are processing alone, but you may be able to by using other information you hold or information you can *reasonably* access from another source."[247] Yet while ALPR data *seems* to meet the requirements of inclusive, subjective, indirectly identifiable data,[248] it is not explicitly mentioned in any GDPR guidelines.

License-plate mapping presents one key point of contention: the public nature of the information gathered. Traditionally, public spaces are not, by definition, private. Therefore, information from license plates on vehicles being driven in public is arguably not personal data. Furthermore, license plates do not automatically tie to an individual. While registration databases allow law enforcement to "reasonably access" who is *likely* driving a car with a specific license plate, owners may lend their car to others, thereby adding an additional level of legal distinction between the license plates and personal data.

---

and public authorities must employ a Data Protection Officer (DPO) to manage compliance with the GDPR. *Id*. Based on these requirements, companies and government entities utilizing ALPR technology must incorporate additional requirements such as informing the public that ALPR technology is in use, complying with both law enforcement requests for data and public requests for their own personal data, and complying with data retention and erasure requirements.

[243] *Id.*

[244] *See, e.g.*, *supra* notes 38-45.

[245] Koch, *supra* note 78.

[246] *Id.*

[247] *Id.*

[248] *Id.*

As the EU has shifted towards more progressive policies safeguarding individual privacy, the U.K. has struggled with how to reconcile the practical possibilities of ALPR technology with the reality of data privacy. This struggle has persisted for at least a decade.[249] ALPR devices were created in the U.K.[250] Since the technology's deployment, lawmakers have responded with a comprehensive array of legislative initiatives.

In 2012, the U.K. adopted data collection and retention policies in its Protection of Freedoms Act.[251] And in 2013, the Home Office drafted a Surveillance Camera Code of Practice that establishes a set of "guiding principles" specifically for the use of surveillance camera systems, including ALPRs.[252] Since 2013, the Surveillance Camera Commissioner has further recognized the special "risk potential for intrusion on citizens" and the need for stronger cybersecurity protections for issues like hacking.[253] Yet even though the policies in the U.K. broadly address issues of personal privacy, they still lack some key protections. Specifically, they do not sufficiently address issues such as ALPR misreads and racial profiling.

Unlike the U.S., which has developed a patchwork approach to the issue of ALPR use, the U.K. has adopted clearer uniform practices that yield a more comprehensive framework.[254] The U.K. policy addresses data retention clearly. In the U.K., records obtained through ALPR use can be retained for two years.[255] Investigators have 90 days to consult the records of ALPR data for "ordinary crimes" and up to one year for

---

[249] *See Met Given Real Time C-Charge Data*, BBC NEWS (July 17, 2007, 11:39 AM), http://news.bbc.co.uk/2/hi/uk_news/politics/6902543.stm [https://perma.cc/ETQ2-MAF7].
[250] Mary Beth Sheridan, *License Plate Readers to be Used in D.C. Area*, WASH. POST (Aug. 17, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/08/16/AR2008081602218.html [https://perma.cc/QPH4-NNNK] (noting that ALPRs were developed to thwart the attacks of the Irish Republican Army).
[251] Protection of Freedoms Act 2012, c. 9 (UK).
[252] HOME OFFICE, SURVEILLANCE CAMERA CODE OF PRACTICE 4, 2013, (UK).
[253] *See* SURVEILLANCE CAMERA COMM'R ANN. REP. 2016/17 (2018).
[254] *See* Koops et al., *supra* note 38.
[255] *Id.* at 673.

"serious investigations" or "major investigations."[256] Additionally, the U.K. is also governed by pro-consumer restrictions from the EU's 2018 enactment of the General Data Protection Plan, which, in particular, limits private use of ALPR technology.[257]

In 2012, the Protection of Freedom Act created a framework to guide the overarching regulation of surveillance technology, including CCTV and other surveillance camera technology, such as ALPRs.[258] The Act directed the Secretary of State to develop a code of practice that could encompass provisions including the use of camera systems and the publication of information obtained by these systems.[259] It also outlined procedural requirements for creating this code of practice.[260]

These concerns were ultimately incorporated into a Surveillance Camera Code of Practice, adopted in June 2013.[261] The purpose of the code is "to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them."[262] The code recognizes that the issue with ALPRs[263] is contradictory: while ALPRs are undoubtedly valuable tools to ensure public safety,[264] they are also rife with the potential for abuse.[265] According to the code:

> That is not to say that all surveillance camera systems use technology which has a high potential to intrude on the right to respect for private and family life. Yet this code must regulate that potential, now and in the future. . .. An individual

---

[256] Koops et al., *supra* note 38, at 673 (Major or serious investigations are defined as blackmail, rape, murder, kidnapping, etc.).
[257] *See GDPR Compliance for ANPR*, *supra* note 242.
[258] *See* Protection of Freedoms Act 2012, c. 9, §§ 29-30 (UK).
[259] *Id.* § 29(3).
[260] *Id.* § 30.
[261] *See* HOME OFFICE, *supra* note 252.
[262] *Id.* § 1.5.
[263] *Id.*, §§ 2.1-2.2 (these sections of the paper refer specifically to ALPRs. However, the Surveillance Camera Code of Practice speaks more generally to "surveillance camera systems"). ALPRs are just one of the technologies covered by the Code.
[264] *Id.* § 2.2.
[265] *Id.*

> can . . . rightly expect surveillance in public places to be both necessary and proportionate with appropriate safeguards in place.[266]

Although the code's primary goal is to address the potential for abusive practices by law enforcement, it recognizes that similar concerns could be raised regarding ALPRs operated by individuals, private businesses, or other public authorities.[267] As such, these other operators are encouraged to adopt this code of practice.[268]

The Code proposes twelve "guiding principles" to safeguard individual privacy expectations.[269] The first four principles involve the development or use of ALPRs, and the last eight relate to the use or retention of captured images.[270] These principles can be briefly categorized as follows:

1) ***Need*** – ALPR use must serve a "legitimate aim" and "pressing [government] need."[271] This need would include "national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others."[272] The key issue is "end user" need, especially when ALPR use relates to investigating criminal activity.[273]
2) ***Review*** – ALPR practices must be reviewed regularly to ensure they are justified.[274] An initial review, and periodic reviews, should analyze whether the technology is disproportionately interfering with privacy expectations.[275]

---

[266] *Id.* § 2.3.
[267] *Id.* § 1.8.
[268] *Id.* § 1.17.
[269] *Id.* § 2.6.
[270] *See id.*
[271] *Id.* § 2.6(1).
[272] *Id.* § 3.1.1.
[273] *Id.* § 3.1.2.
[274] *Id.* § 2.6(2).
[275] *Id.* § 3.2.4.

3) ***Transparency*** – ALPR use must be as transparent as practicable in order to support the idea of "surveillance by consent."[276] People in public should be informed that they are being monitored.[277] ALPR operators must work with the community to ensure that ALPR use is legitimate and reasonable[278] and is fairly applied as to not disproportionately impact certain communities.[279]
4) ***Responsibility and Accountability*** – The parties who are responsible and accountable for the collection and use of ALPR data must be clearly defined.[280] This might necessitate designating an official, but even if more than one person jointly owns or operates the system,[281] or the system is used for multiple purposes,[282] the responsibilities should be clearly articulated.[283]
5) ***Communication*** – Internal policies must be clear and communicated to everyone who is required to comply with them.[284] Ideally, these policies would be part of the professional training for all ALPR users.[285]
6) ***Storage*** – Images should only be stored as necessary and should be deleted once their utility has passed.[286] This guideline declines to provide a hard rule for when data should be deleted, but it notes that the retention period "will vary due to the purpose for the system and how long images and other information need to be retained so as to serve its

[276] *Id.* § 2.6(3).
[277] *Id.* § 3.3.1.
[278] *Id.* § 3.3.2.
[279] *Id.* § 3.3.3.
[280] *Id.* § 2.6(4).
[281] *Id.* § 3.4.2.
[282] *Id.* § 3.4.3.
[283] *Id.*
[284] *Id.* § 2.6(5).
[285] *Id.* § 4.5.3.
[286] *Id.* § 2.6(6).

intended purpose."[287] One reason images could be kept for longer than usual is for active crime investigations.[288]

7) ***Access*** – Access to stored data should be strictly limited.[289] It should only be allowed according to the stated purpose of that ALPR system or if necessary for certain law enforcement purposes.[290] Disclosure to third parties for other reasons should be undertaken with caution so as to safeguard privacy,[291] though this information could be made available from public bodies consistent with the U.K. Freedom of Information Act.[292] Individuals may also request information about themselves.[293]
8) ***Competency*** – ALPR operators should maintain relevant "operational, technical and competency" standards.[294] These standards depend on the particular system being used, but would typically cover system operations and maintenance.[295]
9) ***Security*** – Security measures must safeguard the data collected by ALPRs and deter unauthorized access and use.[296] Operators must have a clear policy regarding access and storage.[297]
10) ***Review*** – The system must be reviewed periodically, and regular reports should be published.[298] The goal of the review is to make sure that ALPR use is still justified.[299] A

[287] *Id.* § 4.6.2.
[288] *Id.* § 4.6.3.
[289] *Id.* § 2.6(7).
[290] *Id.* § 4.7.1.
[291] *Id.* § 4.7.2.
[292] *Id.* § 4.7.6.
[293] *Id.* § 4.7.5.
[294] *Id.* § 2.6(8).
[295] *Id.* § 4.8.1.
[296] *Id.* §§ 2.6(9), 4.9.1.
[297] *Id.* § 4.9.2.
[298] *Id.* § 2.6(10).
[299] *Id.* § 4.10.2.

summary of the review should be made public to increase transparency and accountability.[300]

11) ***Effectiveness*** – ALPRs should be "used in the most effective way to support public safety and law enforcement."[301] "Effectiveness" is judged by the ALPRs ability to help users achieve their intended legitimate purpose.[302] The captured data (including metadata) should be preserved properly so it can serve as evidence in court, if necessary.[303] It also should be easy to share with law enforcement agencies, if that is part of the stated purpose of the system.[304]
12) ***Accuracy*** – Stored information should be accurate and up to date if it will be used to compare against a reference database.[305] ALPR data must be assessed regularly to confirm that it serves the stated purpose of the system.[306] System operators should also adopt a policy to determine when plate numbers should be included in the reference database.[307]

Although the code provides no civil or criminal recourse against any entity that violates it, the code can be admissible in criminal or civil cases stemming from violations.[308] Failure to adhere to the code could be viewed as a dereliction of duty in these cases.[309]

These guidelines overall provide a thorough, flexible framework that balances the need for information and the desire to secure individual privacy. The guidelines recognize the importance of articulating and

---

[300] *Id.* § 4.10.4.
[301] *Id.* § 2.6(11).
[302] *Id.* § 4.11.1.
[303] *Id.* §§ 4.11.2, 4.11.4
[304] *Id.* § 4.11.3.
[305] *Id*. § 2.6(12).
[306] *Id*. § 4.12.1.
[307] *Id*. § 4.12.2.
[308] *Id*. § 1.16.
[309] *Id.*

creating comprehensive clear policies for ALPR use. Information captured by ALPRs should be treated carefully, and collection/use practices must be transparent and clearly communicated to the public. These U.K. guidelines diverge slightly from the bulk of the U.S. statutes because the U.K. guidelines provide no hard-and-fast timeline for the deletion of captured data. However, the U.S. statutes include exemptions for certain law enforcement data, which enable longer retention periods. Since much of the ALPR data is captured and used by law enforcement, this winds up being a divergence with little difference.

## IV. POLICY RECOMMENDATIONS FOR ALPR INTEGRATION

At stake in this discussion is what the global response will be to the privacy concerns raised by new technologies. Contact-tracing, COVID-19, and governmental overreach in 2020 have brought the issue of individual privacy to the forefront. [310] The U.S. state statutes and U.K. code provide an excellent starting place for ALPR policies, but it is important to distill the specific problems and recommendations considering widespread implementation of this technology. The study borrows from both approaches to create a broad approach that guides legislative recommendations.

To that end, this study also draws inspiration from other sources. For example, one main frame related to ALPR technology is addressed by scholars Bert-Jaap Koops, Bryce Clayton Newell and Ivan Škorvánek, "Location Tracking By Police: The Regulation of 'Tireless and Absolute Surveillance.'"[311] These scholars explored a framework to evaluate the relationship between informational and behavioral privacy in the form of location tracking.[312] According to the scholars, this framework was adopted by Italian authors arguing that tracking inherently impacted "liberty of movement": a behavioral privacy

[310] *See generally*, *Examples of Abuse*, PRIVACY INT'L https://privacyinternational.org/examples/tracking-global-response-covid-19 [https://perma.cc/HX7W-XBXA].
[311] Koops et al., *supra* note 38, at 635.
[312] *Id.* at 691.

interest specifically protected by the Italian Constitution.[313] The scholars argue when individuals are tracked, their right to free movement is inexorably constrained. While this approach to privacy has mainly been limited to Italian law, the scholars note that the approach has also emerged in other contexts, including U.S. scholarship.[314]

This section concludes that ALPR technology should be regulated via a comprehensive federal statute that secures individual privacy and provides significant individual control over the collection and use of ALPR data. To this end, there are seven broad areas that should be addressed in statutory construction:

### *A. Who Needs the Data, and How Is That Need Demonstrated?*

As a threshold matter, ALPR use should serve a legitimate aim,[315] which could encompass national security, public safety, or crime.[316] Pertinent statutory guidelines must clarify what constitutes "need" for the data collected for a particular legitimate aim. The legislation must additionally address what entities can assert "need" for ALPR data. Is "need" limited to law enforcement, or can private entities also claim authority to use ALPR technology?

As noted above, there is significant debate regarding this question. This study ultimately argues that the use of ALPR technology should be restricted to law enforcement agencies engaging in "legitimate law enforcement purposes."[317] The broad deployment of ALPR technology by private entities entails a privacy invasion that outweighs the benefits of the technology. However, restrained use of ALPR technology by law enforcement is critical for public safety and investigative purposes.

---

[313] *Id.*
[314] *Id.* at 692 (noting that U.S. scholar William Herbert has argued that location monitoring is "a vestige and incident of slavery" that raises Thirteenth Amendment concerns).
[315] HOME OFFICE, *supra* note 252, at § 2.6(1).
[316] *Id.* § 3.1.1.
[317] As an example, in the U.S. state of Maryland, this is defined as "the investigation, detection, or analysis of a crime or a violation of the Maryland vehicle laws or the operation of terrorist or missing or endangered person searches or alerts." *See, e.g.*, MD. CODE ANN., PUB. SAFETY § 3-509(a)(8) (West 2019).

The key is how to reasonably restrain law enforcement use of ALPRs, balancing the public's interest in privacy against law enforcement's need for data. Language from the Arkansas ALPR statute is instructive here; it makes it illegal for "an individual, partnership, corporation, association" or Arkansas state agencies to use ALPRs.[318] ALPR use is limited to law enforcement agencies for specified purposes, including ongoing investigations and verification of registration data.[319] These limitations restrain the abusive practices – broad deployment and surveillance – facilitated by ALPR technology. Legislation should include clearly defined examples of "legitimate" purposes warranting ALPR use.[320]

A further limitation on data collection and use can be found in Minnesota's statute.[321] The statute has two important components. First, it limits the types of data that can be collected to license plate numbers, date/time/location data and pictures of vehicles and areas in the immediate vicinity.[322] Second, it restricts the databases against which the data can be checked.[323] These limitations reasonably constrain the broad deployment of ALPRs, reduce the motivation for abusive data collection practices, and help secure individual privacy.

Furthermore, within the context of law enforcement use, there should be a clear distinction between the use of mobile ALPRs affixed to police cruisers and stationary ALPRs affixed to structures such as utility poles.

Mobile ALPRs, associated with police movement, patrol, and action, arguably pose less of a privacy risk to individuals because the data is collected in an active state. Stationary ALPRs, on the other hand, are akin to closed circuit television surveillance (CCTV). Although CCTV technology is widely accepted, particularly in highly surveilled

---

[318] ARK. CODE ANN. § 12-12-1803 (West 2013).
[319] ARK. CODE ANN. §§ 12-12-1801 to 1808 (West 2013). *See also,* ARK. CODE ANN. § 12-12-1803 (West 2013) (enabling parking enforcement entities to use ALPRs).
[320] *See, e.g.*, VT. STAT. ANN. tit. 23, § 1607(c) (West 2018) (limiting the use of ALPRs to "legitimate law enforcement purposes").
[321] MINN. STAT. ANN. § 13.824(2) (West 2015).
[322] *Id.* § 13.824(2)(a).
[323] *Id.*

locations such as the U.K., the governmental creation of a massive, traceable database of license plates threatens individual privacy. Thus, while mobile ALPRs may have a lower bar for implementation, law enforcement should demonstrate increased need before deploying stationary ALPRs. For example, if law enforcement has ample evidence that an area is routinely the site of drug trafficking (or another geographically specific crime), it may demonstrate a heightened need for deploying stationary ALPR technology, perhaps affixed to a light pole in the area.

As a component of establishing need, any use of ALPRs should have a mandated review period. Taking a page out of the U.K.'s policies, there should be an initial review, and periodic reviews, that focus specifically on privacy expectations of citizens for the country in question.[324]

### *B. How Is Transparency Obtained and Communicated?*

The ultimate goal should be "surveillance by consent."[325] To that end, government entities should be transparent regarding their surveillance practices. For stationary ALPRs, there should be a public sign clearly informing people they are being monitored.[326] Mobile ALPRs attached to police cruisers or official vehicles should have a similar notice, a practice already implemented for many dashcam recorders and bodycam operations by U.S. police forces.[327]

ALPR use policies must also be clearly communicated in writing to the public before deployment of the technology. This provision is critical because it gives the public advance notice that ALPRs will be used, and it increases the likelihood of buy-in. The Montana statute is an excellent model here because it requires law enforcement agencies to provide written policies and publicize them before using ALPR technology.[328]

---

[324] HOME OFFICE, *supra* note 252, § 3.2.4.
[325] *Id.* § 2.6(3).
[326] *Id.* § 3.3.1.
[327] *See, e.g.*, 50 ILL. COMP. STAT. 706 / 99-352 (2016); General Orders, AUSTIN POLICE DEP'T. § 303 (Nov. 1, 2018).
[328] MONT. CODE ANN. § 46-5-117(d) (West 2017).

### *C. How Is Accountability Ensured?*

There must be a strict level of accountability, with a clear mechanism for the public to identify responsible parties and hold them accountable for any surveillance misconduct. Due to the special concerns of ALPRs being used to target communities of color or other groups traditionally at risk for profiling and/or state mandated violence, it is especially important that these databases of information be managed openly and effectively.

Any government entity using ALPRs should have internal employees who are responsible and accountable for the collection and use of ALPR data.[329] If the government entity gathers other public information (through, for example, bodycam footage, CCTV footage, or drone footage), it would make sense to designate this as a singular position. Additionally, there must be some sort of ombudsman channel for the public to register complaints about profiling, mishandling of ALPR information, etc. Relevant to the standards of the country in question, it would be appropriate to incorporate civil and/or criminal consequences for the misuse of ALPR data. Criminal penalties, such as those adopted in Maryland and Georgia, arguably encourage modest, targeted data collection practices, reining in the abusive practices identified in connection with ALPR technology.

Furthermore, legislation should incorporate specific audit requirements that empower the public to serve as a critical "check" on the efficacy and ethics of the particular data collection practices. These guidelines should follow states such as Minnesota, Montana, New Hampshire, and Vermont, which have established for periodic audits of ALPR technology.[330]

### *D. For How Long Can ALPR Images Be Stored?*

Long-term storage of ALPR images is one of the most contentious aspects of this technology. The ability to create stable, detailed tracking

---

[329] HOME OFFICE, *supra* note 252, § 2.6(4).

[330] MONT. CODE ANN. § 46-5-117(d)(ii) (2021); N.H. REV. STAT. ANN. § 261:75-b(X) (LexisNexis 2021); VT. STAT. ANN. tit. 23, § 1607(e)(1) (2021); *See*, MINN. STAT. ANN § 13.824(6)(a) (2021).

of non-criminal citizens is something that runs counter to most countries' approach to individual privacy.[331] As evidenced in the U.S. state statutory provisions above, data retention timelines vary wildly.[332] There should be a clearly defined timeframe in the statute that protects privacy and enables law enforcement to achieve their narrowly defined goals.

While this paper acknowledges that certain *types* of use (such as for criminal investigations) may demonstrate the need for long-term retention of ALPR images, the default statutory position should require routine and immediate deletion of ALPR images. In other words, unless ALPR images are part of an existing, active crime investigation, they should be deleted immediately.[333] This provision is found in states like New Hampshire, which require quickly purging ALPR data from the system "unless an alarm resulted in an arrest, a citation, or protective custody, or identified a vehicle that was the subject of a missing person or wanted broadcast."[334]

Along this line, mobile ALPR data is more likely to be maintained for longer periods, because it is more likely to be gathered in pursuance of an actual crime. This data should be subject to a reasonable retention policy; the U.S. statutes have settled on various timeframes, with 90 days being the most frequent.[335] In contrast, stationary ALPR data should be deleted more quickly, as it serves as passively gathered metadata. One of the main goals in this provision should be to reduce the use of ALPR data for analytic purposes.

Legislation should also incorporate provisions extending these timeframes in certain narrowly defined circumstances. Here, the data could be retained longer if it is being used as evidence, subject to a

---

[331] *See, e.g.*, U.S. CONST. amend. IV.
[332] MONT. CODE ANN. § 46-5-118(1) (2021); N.H. REV. STAT. ANN. § 261:75-b(VIII) (LexisNexis 2021); VT. STAT. ANN. tit. 23, § 1607(d)(2) (2021); *See*, MINN. STAT. ANN § 13.824(3)(a) (2021).
[333] HOME OFFICE, *supra* note 252, § 4.6.3.
[334] N.H. REV. STAT. ANN. § 261:75-b(VIII) (2016).
[335] *See, e.g.*, MONT. CODE ANN. §§ 46-5-117 to -119 (2017); N.C. GEN. STAT. § 20-183.30 to -183.32 (2015); TENN. CODE § 55-10-302 (2014).

criminal investigation, or is the center of a preservation request or search warrant.

### *E. Who Can Access ALPR Data?*

Access to stored data should be strictly limited to the government entity that gathered it.[336] There should be an appropriate exception for law enforcement purposes; these purposes would vary from country to country.[337] For example, different law enforcement branches in the U.S. have different, sometimes overlapping, jurisdictions.[338] One law enforcement branch could justifiably be expected to share pertinent ALPR data about a crime with another law enforcement branch. This exemption should be specifically built into the statute.[339]

The statute should clearly reflect that there should be no sale or transmission of ALPR data to third parties.[340] Individuals, however, should be able to request any stored data about themselves. The data also could reasonably be disclosed when legally necessary, such as in the context of court orders or regulatory requirements.

### *F. How Is ALPR Data Secured, and What Are the Consequences of Inadequate Security?*

The security of government-held data is an evolving area of concern. Data costs can be prohibitive to many government agencies.[341] Quick deletion of content is one way to balance the cost of data storage with data security. Currently government entities have responded in the U.S. in two ways: first, by keeping storage internal, sometimes with inadequate security protections, and second, by outsourcing data storage

---

[336] HOME OFFICE, *supra* note 252, § 2.6(7).
[337] *Id.* § 4.7.1.
[338] *See* MONT. CODE ANN. § 44-2-115 (2021); S.C. CODE ANN. § 23-1-212(B) (2021).
[339] *See, e.g.*, ARK. CODE ANN. § 12-12-1804(d)(2) (2013) (allowing data to be shared with other law enforcement agencies when evidence of an offense is uncovered).
[340] *See., e.g.*, CAL. VEH. CODE § 2413(c) (West 2021) (restricting the California Highway Patrol from selling ALPR data for any reason or providing the data to non-law enforcement parties).
[341] *See Why Data Growth Poses a Challenge for Government Agencies*, DSM (Apr. 17, 2019), https://www.dsm.net/it-solutions-blog/why-data-growth-poses-a-challenge-for-government-agencies [https://perma.cc/ZBG8-NCMF].

to a third-party company, who occasionally monetize the data.[342] The specifics of ALPR data storage should be reviewed periodically to ensure the latest security improvements are incorporated. Operators must have a clear policy regarding access and storage, regardless of what the current industry standard is regarding security.[343] Additionally, the government should be held liable for any data theft.

### *G. How Should ALPR Data Collection and Retention Practices Be Reviewed?*

To ensure that data collection and retention practices are fair and transparent, this study recommends following the model of the U.S. state of Arkansas. Arkansas law mandates that statistical data be compiled and reviewed every six months in a format suitable for public review.[344] The data is limited, including only the following: how many license plates were scanned, the names of the lists these plates were checked against, the number of matches made, the number of matches that were found to be benign, and the number of matches that led to an arrest.[345]

## V. CONCLUSION

Given the significant privacy concerns raised with the widespread adoption of ALPRs, it is imperative to craft comprehensive policies that safeguard individual privacy. A comparison of U.S. and U.K. approaches reveals differing levels of protection. While the U.K. has embraced comprehensive privacy protections, the U.S. has tended to defer to the states and local regulations. The result is patchwork legislation that fails to protect individual privacy adequately.

The study ultimately asserts that comprehensive consumer-centric federal legislation should be adopted to secure privacy. By synthesizing emerging themes in the U.K. and the U.S., the study recommends seven broad policies that should be captured in the legislation:

---

[342] *See id.*
[343] HOME OFFICE, *supra* note 252, §4.9.2.
[344] ARK. CODE ANN. § 12-12-1805(a)(1) (2013).
[345] *Id.* § 12-12-1805(b).

- Who needs the data, and how is that need demonstrated?
- How is transparency obtained and communicated?
- How is accountability ensured?
- For how long can ALPR images be stored?
- Who can access ALPR data?
- How is ALPR data secured, and what are the consequences of inadequate security?
- How should ALPR data collection and retention practices be reviewed?

Incorporating these seven policies into the regulation has two benefits: first, it helps secure individual privacy, and second, it enables restrained, targeted use of ALPR technology by law enforcement to achieve legitimate, narrowly defined law enforcement purposes. The resulting legislation thus addresses both law enforcement's asserted need for surveillance tools and individual expectations regarding privacy.